ネットワーク認証アプライアンス

取扱説明書　Ver 4.4.0

Rev. 20150810

アイビーソリューション株式会社

目次

1　はじめに

iBAQS-FX をお買い上げいただき、ありがとうございます。

本取扱説明書では、正しい使い方やご注意いただきたい内容や参照ページを記載しています。

ご使用前に本書をよくお読みください。

1.1　本書の見かた

本書の対象読者

iBAQS-FX を利用したネットワークを構築したり運用を行ったりする方を対象としています。

本書の構成

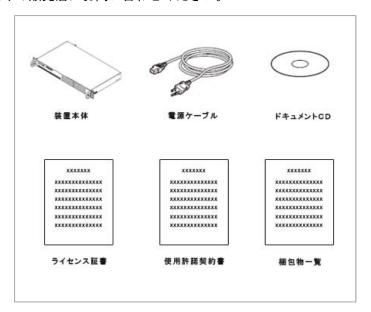
本書の構成は以下の通りです。

概要	iBAQS-FX の特長やハードウェア仕様について説明します。
動作環境	動作環境について説明します。
導入	導入方法について説明します。
運用	運用方法について説明します。
保守	保守について説明します。
困った時には	困った時の対処方法について説明します。

本書で使用しているマーク

	お使いになる上で注意していただきたい点やしてはいけない点を記載しています。
	知っておくと便利なことや関連知識などを記載しています。

1.2 内容物に関して（アプライアンス版）

ご使用の前に、次のものがそろっているかご確認ください。万一、不足しているものがあった場合は、お買い上げの販売店にお問い合わせください。

□ 装置本体	□ ライセンス証書
□ 電源ケーブル	□ ドキュメントＣＤ
□ 使用許諾契約書	□ 梱包物一覧

1.3 内容物に関して（仮想アプライアンス版）

ご使用の前に、次のものがそろっているかご確認ください。万一、不足しているものがあった場合は、お買い上げの販売店にお問い合わせください。

□ インストールメディア	□ ライセンス証書
□ 使用許諾契約書	□ 梱包物一覧

1.4 著作権について

1.5 安全にお使いいただくために

本製品を安全にご使用いただくために、以下の記載内容を必ずお守りください。

⚠ 異常が発生したら

煙が出たり変な音がしたりするなどの異常が発生した場合は、直ちにケーブルを装置から抜いた後、販売会社にご相談ください。そのまま使用すると火災や感電の原因になります。

⚠ 破損した電源ケーブルを使用しないでください

火災や感電の原因になります。電源ケーブルを取り扱う際には、以下の点に注意してください。

- 濡らしたり、加工したり、結んだり、束ねたり、巻きつけたりしない
- 重いものを載せたり、ドアなどにはさんだり、落下させたり、衝撃を与えたりしない
- 引っ張ったり、無理に曲げたり、ねじったりしない
- 電源ケーブルのプラグに金属を近づけない
- 熱器具のそばで使わない

電源ケーブルが破損した場合は、ただちに使用を中止し、販売会社にご相談ください。そのまま使用すると火災や感電の原因になります。

⚠ 雷があったときはケーブル類・機器類にさわらないでください

感電の原因となります。

⚠ 通風口をふさがないでください

火災の原因となります。

⚠ 湿気やほこりの多いところには置かないでください

火災や感電の原因となります。

強い磁気やノイズ発生源から離して設置してください

誤動作の原因となります。

通路にケーブルをはわせないでください

つまずいてけがの原因となります。

機器の上に重いものを載せないでください

ものが落下したり、装置が転倒したりしてつまずいてけがの原因となります。

表示以外の電圧では使用しないでください

火災や感電の原因となります。

電波障害自主規制について

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。
VCCI-A

使用上の注意

- 本製品は、お客さまの責任でご使用ください。
- 本製品の使用によって発生する損害やデータの損失については、アイビーソリューション株式会社は一切その責任を負いかねます。また、本製品の障害の保障範囲はどんな場合においても、本製品の代金としてお支払いいただいた金額を超えることはありません。あらかじめご了承ください。
- 本製品に、改変や分解を行うことを一切許可しておりません。
- このソフトウェアの仕様は、改良のため予告なく変更する場合がありますが、ご了承ください。

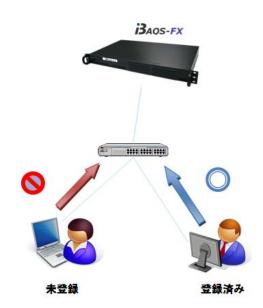
Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

その他、本書で登場するシステム名、製品名は、一般に各開発メーカーの登録商標あるいは商標です。

2 概要

iBAQS-FX の概要を説明します。

2.1 iBAQS-FX について

iBAQS-FX は RADIUS 認証サーバです。情報漏えいや不正アクセスによる信頼の失墜を防ぎ、正しいアクセスを徹底して、強固で安定したネットワーク環境を構築する認証システムです。 当システムでは導入も容易にわかりやすい管理画面で管理者の負担を軽減します。

2.2 iBAQS-FX の特長

iBAQS-FX には、以下の特長があります。

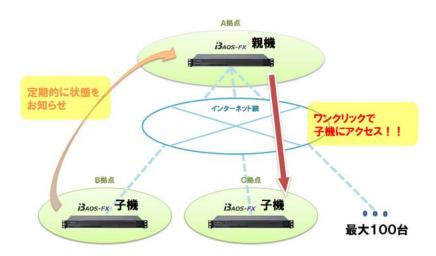
① ７つの認証パターン

次の７つの認証パターンを利用できます。プリンターなどの機器や端末を限定したい場合は、MAC アドレス認証、人を限定したい場合はユーザーID 認証、端末と人を限定したい場合はより強固な組み合わせ認証（ユーザーID ＆ MAC アドレス認証）を利用し、運用場面に合った認証パターンを選択することが可能です。

※ワンタイムパスワード認証で利用可能な認証方式は PAP のみとなります。IEEE 802.1X 認証では利用できません。

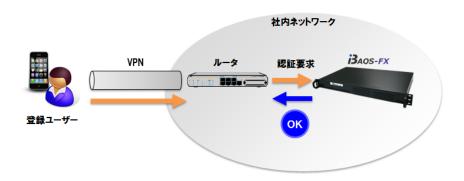
認証パターン
MAC アドレス認証
ユーザーID 認証
クライアント証明書認証
ユーザーID ＆ MAC アドレス 認証
クライアント証明書 ＆ MAC アドレス 認証
ワンタイムパスワード認証
ワンタイムパスワード ＆ MAC アドレス 認証

② ストップ防止の冗長構成や集中管理

障害が発生した場合に認証が止まってしまうことを防止するため、冗長構成に対応しています。また、複数拠点に配置させた iBAQS-FX（子機）を１台の iBAQS-FX（親機）で集中管理することができます。

③ 不正アクセス場所の特定

どの場所から不正アクセスが行われたのかを特定することが可能です。 いつ、どのスイッチの、どのポートに接続されたのかを確認することで、速やかに対応することができます。

④ スマートフォンからのリモート接続認証

スマートフォンなどから社内ネットワークに認証接続させることができます。

⑤ 登録作業を軽減するMAC収集モードと事前登録

MAC 収集モードを利用することにより、自動で MAC アドレスを収集し一括登録することが可能です。また、利用者に事前登録を行ってもらい、承認許可することで登録することも可能です。

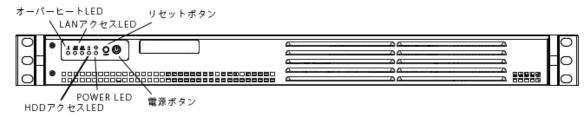
2.3 iBAQS-FX のハードウェア仕様（アプライアンス版）

iBAQS-FX のハードウェア仕様は以下の通りです。

スペック一覧

CPU	インテル® Atom™プロセッサー N2800 1.8GHz
メモリ	4GB
HDD	500GB
通信速度	10Mbps/100Mbps/1000Mbps
ポート	ネットワーク：RJ-45 x 2（GbE)、 USB：USB 2.0 x 2、USB 3.0 x 2
形状	小型 1U ラックマウント
外形寸法	437（W）x 249（D）x 43（H）mm （突起部含まず）
重量	3.7kg
電源	定格入力電圧 ： 100 - 240 V 定格周波数 ： 50 - 60 Hz 最大入力電流：2.6A
最大消費電力	46.1W
最大発熱量	165.96kj/h
環境	動作時温度：10 ℃ ～ 35 ℃ 動作時湿度： 8 % ～ 90 %(但し結露しない事) 保管時温度：-40 ～ 70℃ 保管時湿度：5 ～ 95 %(但し結露しない事)
適合規格	VCCI Class A、RoHS

各部名称と働き

[前面]

(1) オーバーヒート LED

オーバーヒート状態にあるときに点灯します。点灯した場合には周囲のエアフローを確認してください。

(2) LAN アクセス LED

ネットワークアクセス時に点灯します。

(3) HDD LED

内蔵ハードディスクドライブのアクセス時に点灯します。

(4) POWER LED

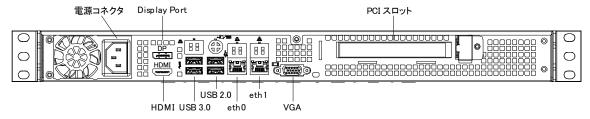
本機の通電状態を表示します。

(5) リセットボタン

押すとリセットを実行します。通常は使用しないでください。

(6) 電源ボタン

電源を ON/OFF するスイッチです。一度押すと POWER ランプが点灯して ON の状態になります。4 秒以上押し続けると強制的に電源を切ることができます。通常はウェブの管理画面から電源を切ってください。

[背面]

(1) 電源コネクタ

AC コードを接続するコネクタです。

(2) Display Port

Display Port に対応している機器と接続します。

※本機では使用しません

(3) HDMI

HDMI に対応している機器と接続します。

※本機では使用しません

(4) USB 3.0

USB 3.0 インターフェースに対応している機器と接続します。

※本機では使用しません

(5) USB 2.0

USB 2.0 インターフェースに対応している機器と接続します。

※本機では UPS との接続に使用します

(6) VGA

ディスプレイを接続できます。

※運用時には使用しません

(7) eth0

1000BASE-T/100BASE-TX/10BASE-T と接続するコネクタ

(8) eth1

1000BASE-T/100BASE-TX/10BASE-T と接続するコネクタ

(9) PCI スロット

PCI カードを装着する差し込み口です。

※本機では使用しません

2.4 iBAQS-FX の要求仕様（仮想アプライアンス版）

iBAQS-FX の要求仕様は以下の通りです。

要求仕様一覧

ハイパーバイザー	VMware ESXi 5.1/5.5/6.0
メモリ	512MB 以上の割当て
ストレージ	64GB 以上の空き

ネットワークアダプタの追加、削除はシステムエラーが発生したり、仮想アプライアンスへの通信が行えなくなる可能性があり、サポートされませんのでご注意ください。

3 動作環境

iBAQS-FX を利用する環境において、各機器に必要な環境について説明します。

iBAQS-FX 環境では、認証を行う当筐体 iBAQS-FX、認証スイッチ、クライアントで構成されます。

3.1 クライアント環境

OS	制限なし
その他条件	IEEE802.1X 認証ではサプリカントが必要になる場合があります ※Windows 標準機能でも利用可能です。

3.2 管理画面にアクセスする機器

iBAQS-FX の管理画面は Web ブラウザで利用可能なため、Web ブラウザが必要となります。

OS は以下のブラウザをサポートする OS とします。

- Internet Explorer 8 以降
- Mozilla Firefox 3.5 以降

➢ 使用する Web ブラウザでは、JavaScript を利用できるように設定してください。

3.3 対応スイッチ

本製品に対応するネットワーク機器は次の通りです。

2013年5月現在

アライドテレシス	[レイヤー3] SwitchBlade x908　AT-x600-48Ts AT-x900-24XT　AT-x600-48Ts/XP AT-x900-24XS　AT-x600-24Ts AT-x900-12XT/S　AT-x600-24Ts/XP CentreCOM 8948XL　AT-x600-24Ts-POE AT-x610-48Ts/X-POE+　AT-x510-52GTX AT-x610-24Ts/X-POE+　AT-x510-28GTX AT-x610-48Ts/X　CentreCOM 9424T AT-x610-24Ts/X　CentreCOM 8748SL CentreCOM 8724SL V2 [レイヤー2] CentreCOM 9408LC/SP　AT-x210-24GT CentreCOM 8424XL　AT-x210-16GT CentreCOM 8424TX　AT-x210-9GT CentreCOM 8324XL　CentreCOM 9048XL CentreCOM 8316XL　CentreCOM GS900M V2 シリーズ AT-x200-GE-28T　CentreCOM FS900M シリーズ AT-x200-GE-52T
ジュニパーネットワークス	SA シリーズ
エクストリーム　ネットワークス	Summit シリーズ
エクストリコム	EXSW シリーズ
その他	認証スイッチ　（RADIUS 認証可能なスイッチ）

●SwitchBlade、CentreCOM はアライドテレシスホールディングス株式会社の登録商標です。

3.4 対応 UPS

本製品に対応する UPS は次の通りです。

2012 年 11 月現在

APC	Smart-UPS CS シリーズ ES シリーズ RS シリーズ

3.5 対応ワンタイムパスワードトークン

本製品に対応するワンタイムパスワードトークンは次の通りです。

2013 年 5 月現在

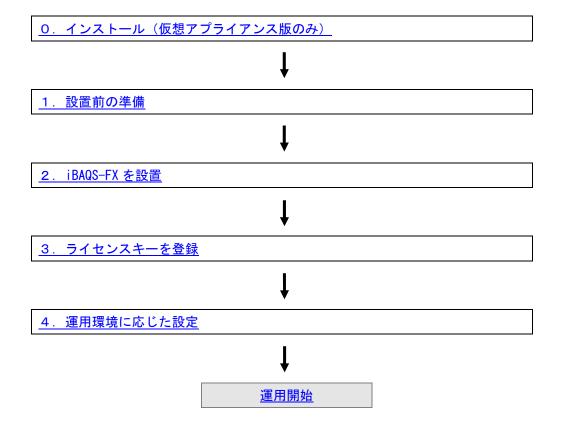
飛天ジャパン	C200(ハードウェア)
Archie L. Cobbs	OATH Token(ソフトウェア、iOS 向け)
Bite The Bullet	Android Token(ソフトウェア、Android 向け)

- ワンタイムパスワード認証で利用可能な認証方式は PAP のみとなります。IEEE 802.1X 認証では利用できません。

4 導入

iBAQS-FX の導入について説明します。

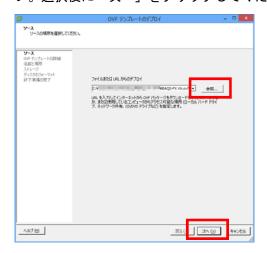
4.1 導入手順

導入手順は以下の通りです。

4.2 インストール（仮想アプライアンス版）

iBAQS-FX を導入する VMware ESXi サーバをご用意ください。本項では vSphere Client を用いたインストール手順を説明します。vSphere Client を導入した PC に ovf ファイル一式を配置してください。

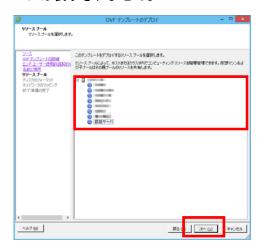
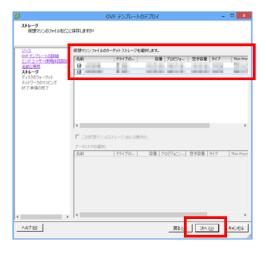
【手順】

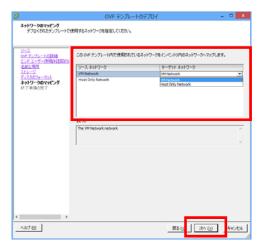
1. vSphere Client でインストール対象の ESXi サーバに接続します。
2. メニューバーのファイルメニューから「OVF テンプレートのデプロイ」をクリックしてください。

3. 『ソース』が表示されます。「参照」ボタンをクリックして ovf ファイルを選択してください。選択後に「次へ」をクリックしてください。

4. 『OVF テンプレートの詳細』が開きます。内容を確認して「次へ」をクリックしてください。

5. 『エンドユーザー使用許諾契約書』が表示されます。使用許諾契約書の内容を確認して、「承諾」ボタンをクリックして、「次へ」ボタンをクリックしてください。

6. 『名前と場所』が表示されます。他の仮想マシンに重複しない名前を入力して、「次へ」をクリックしてください。

7. 『リソースプール』が表示されます。仮想マシンを作成するリソースプールを選択して、「次へ」をクリックしてください。
   ※リソースプールが存在しない場合、リソースプールを選択してデプロイを開始した場合には表示されません。

8. 『ストレージ』が表示されます。仮想マシンを作成するデータストアを選択して、「次へ」をクリックしてください。
   ※データストアが１つの場合には表示されません。

9. 『ディスクのフォーマット』が表示されます。プロビジョニング方式を選択して、「次へ」をクリックしてください。
   ※ディスクプロビジョニングはシックプロビジョニングを推奨します。

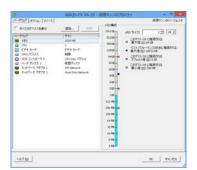
10. 『ネットワークのマッピング』が表示されます。eth0 と eth1 のターゲットネットワークを選択して、「次へ」をクリックしてください。
   ※eth0 と eth1 は異なるネットワーク(仮想スイッチ)に接続されることを推奨します。

11. 『終了準備の完了』が表示されます。「終了」ボタンをクリックしてください。

12. デプロイが始まります。10 分程度で完了します。

13. デプロイが完了します。「閉じる」をクリックしてください。

14. デプロイした仮想マシンを選択して、「仮想マシン設定の編集」をクリックしてください。

15. 用途に応じてメモリ、CPU の設定を調整してください。

既定値はメモリ：1GB、CPU：仮想ソケット数 1、ソケットあたりのコアの数 2 です。

16. 仮想マシンの電源を入れてください。iBAQS-FX を操作するには iBAQS-FX と同じセグメントに設定用 PC を接続し、ネットワーク設定を行い、ブラウザで【http://192.168.1.1:10080/】へアクセスしてください。iBAQS-FX の初期設定は次項の手順 4 以降をご確認ください。

4.3 設置前の準備

iBAQS-FX を設置する前に iBAQS-FX の IP アドレスの設定を行います。そのため、コンピュータ（以降、設定用 PC と表記）を準備します。設定用 PC には、Web ブラウザが必要です。

【手順】

1. iBAQS-FX の eth0 LAN コネクタ（背面向って左側）に LAN ケーブルを差し込みます。

➢ 使用する LAN ケーブルは、ストレートケーブルでもクロスケーブルでも構いません。

2. 設定用 PC に LAN ケーブルを差し込みます。
3. iBAQS-FX の電源ケーブルを差し込みます。POWER LED ランプがグリーン点灯となります。

➢ 電源ケーブルを接続した段階で、起動します。

4. iBAQS-FX の初期 IP アドレスが「192.168.1.1」であるため、設定用 PC の IP アドレスを次のように設定し、iBAQS-FX とネットワーク接続ができるようにします。

【設定用 PC の IP アドレス設定例】

IP アドレス	192.168.1.254
サブネットマスク	255.255.255.0

5. 設定用 PC の Web ブラウザから以下の URL にアクセスします。

```
http://192.168.1.1:10080/
```

⇒ログイン画面が表示されます。

6. 管理者 ID とパスワードを入力して[ログイン]ボタンをクリックします。

【デフォルト管理者 ID、パスワード】

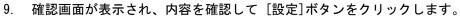
管理者 ID	manager
パスワード	friend

7. ログインが成功すると、トップ画面が表示され、[サーバ設定]をクリックします。

8. サーバ設定画面<<基本タブ>>が表示されます。設置環境に応じて入力し、[設定]ボタンをクリックします。

サーバ設定<<IP アドレスタブ>>画面の項目

番号	画面項目	説明
(1)	使用 LAN インターフェース	使用するインターフェースです。 eth0 または eth1 を選択します。
(2)	eth[n] MAC アドレス	eth[n]の MAC アドレスです。
(3)	eth[n] 使用	eth[n]の使用状態です。
(4)	eth[n] IP アドレス	eth[n]の IP アドレスです。 入力制限）IP アドレス形式 例）192.168.1.100
(5)	eth[n] サブネットマスク	eth[n]のサブネットマスクです。 入力制限）IP アドレス形式 例）255.255.255.0
(6)	デフォルトゲートウェイ	サーバのゲートウェイです。 入力制限）IP アドレス形式　必須 例）192.168.1.254
(7)	ホスト名	サーバのホスト名です。 入力制限）半角英数字,'-','_'　32 文字以内　必須
(8)	セッションタイマー時間	セッションタイマー時間です。 管理画面の無操作によるタイムアウト時間を設定します。 入力制限）1 分～99 分　必須
(9) ～ (11)	DNS	DNS です。 オンラインでのライセンス設定、アップデート機能をご利用いただくためには DNS の設定が必須です。 入力制限）IP アドレス形式 例）192.168.1.252
(12) ～ (15)	タイムサーバ	NTP サーバです。 iBAQS-FX が時刻同期に使用する NTP サーバを設定します。
(16) (17)	プロキシサーバ	プロキシサーバです。 iBAQS-FX がアップデートサーバと通信する際に使用するプロキシサーバを設定します。

9. 確認画面が表示され、内容を確認して［設定］ボタンをクリックします。

10. 完了画面が表示されます。

11. 再度、IP アドレス変更後の iBAQS-FX にアクセスするため、設定用 PC の IP アドレスを iBAQS-FX と同じネットワークの IP アドレスに変更します。

【設定用 PC の IP アドレス設定例】

iBAQS-FX の IP アドレス	192.168.10.100
iBAQS-FX のサブネットマスク	255.255.255.0
設定用 PC の IP アドレス	192.168.10.254
設定用 PC のサブネットマスク	255.255.255.0

12. 設定用 PC の Web ブラウザから以下の URL にアクセスし、ログインします。

http://<iBAQS-FX の IP アドレス>:10080/

13. ログイン後、再度サーバ設定画面<シャットダウンタブ>に遷移し、[シャットダウン]ボタンをクリックします。

[ログイン]→[トップ]→[サーバ設定]<<シャットダウンタブ>>

14. 確認画面が表示され、[はい]ボタンをクリックします。

15. 完了画面が表示され、iBAQS-FX がシャットダウンします。

以上で設置前の準備は完了です。

4.4 iBAQS-FX を設置

IP アドレスの設定が完了した iBAQS-FX を運用環境に設置します。

【手順】

1. ネットワーク上のスイッチに iBAQS-FX を LAN ケーブルでつなぎます。
2. iBAQS-FX の電源ケーブルを差し込みます。POWER LED ランプがグリーン点灯となります。

> ➢ 電源ケーブルを接続した段階で、起動します。

3. 管理 PC の Web ブラウザから以下の URL にアクセスし、ログインします。

```
http://<iBAQS-FX の IP アドレス>:10080/
```

4. iBAQS-FX が問題なく動作しているかをトップ画面で確認します。

   [ログイン]→[トップ]

   ⇒インフォメーションに「現在、正常に動作しています。」と表示されていることを確認してください。

> ➢ 異常の場合は、お買い上げの販売店までお問い合わせください。

トップ画面

以上で iBAQS-FX の設置は完了です。

4.5　ライセンスキーを登録

iBAQS-FX のライセンスキーを登録します。ライセンスキーは、ライセンス証書に記載されております。ライセンスキーの登録では、オンラインとオフラインの２パターンでの登録が可能です。

- オンラインライセンスキー設定の場合、iBAQS-FX がインターネットに接続可能である必要があります。また、設定した DNS が正しく名前解決ができる必要があります。
- オフラインライセンスキー設定の場合、インターネットに接続可能な環境である必要はありません。オフラインライセンスキー設定を行いたい場合は、オフライン用ライセンス設定ファイルが必要です。オフライン用ライセンス設定ファイルご希望の場合は、アイビーソリューションまたはお買い上げの販売店にお問い合わせください。

オンラインライセンスキー設定

オンラインでライセンスキーを設定します。

【手順】

1.　iBAQS-FX の管理画面にアクセスし、ライセンス設定画面≪オンラインタブ≫を表示します。
　　[ログイン]→[トップ]→[ライセンス設定] ≪オンラインタブ≫
　　ライセンス証書のライセンスキーを入力し、[設定]ボタンをクリックします。

2. 完了画面が表示され、再度ライセンス設定画面≪オンラインタブ≫を表示し、ライセンス情報が登録されたことを確認します。

オンラインでの登録は以上です。

オフラインライセンスキー設定

オフラインでライセンスキーを設定します。

【手順】

1. オフライン用ライセンス設定ファイルをアイビーソリューション（株）から入手します。
2. 入手したファイルを管理 PC のデスクトップに保存します。
3. iBAQS-FX の管理画面にアクセスし、ライセンス設定画面<<オフラインタブ>>を表示します。
   [ログイン]→[トップ]→[ライセンス設定]<<オフラインタブ>>
   オフライン用ライセンス設定ファイルを選択し、[設定]ボタンをクリックします。

4. 再度システム設定画面<<ライセンスタブ>>を表示し、ライセンスキーが登録されたことを確認します。※上記オンラインライセンス設定[2]参照

以上でライセンスキーの登録は完了です。

仮想アプライアンス版ライセンスキー設定

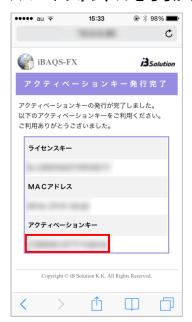
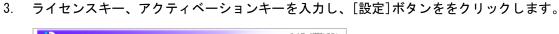
仮想アプライアンス版のライセンスキーを設定します。

【手順】

1. iBAQS-FX の管理画面にアクセスし、ライセンス設定画面に表示されている MAC アドレスをメモします。

2. 【http://ibaqs-fx.ib-sol.co.jp/cgi-bin/ibaqsfx-key.cgi】へアクセスし、アクティベーションキーを取得します。

   スマートフォン、PC どちらからでもご利用頂けます。

3.　ライセンスキー、アクティベーションキーを入力し、[設定]ボタンををクリックします。

4.　完了画面が表示され、再度ライセンス設定画面を表示し、ライセンス情報が登録されたことを確認します。

試用版では有効期限内のライセンスキーのみ設定可能です。また有効期限が切れると利用できなくなりますのでご了承ください。

以上でライセンスキーの登録は完了です。

4.6 運用環境に応じた設定

iBAQS-FX を運用環境に応じた設定を行います。

1. サーバ設定
    - IP アドレス設定
    - 時刻設定
    - 再起動
    - シャットダウン
2. 冗長化設定
3. システム設定
    - モード切り替え
4. ライセンス設定
5. 外部連携設定
    - syslog サーバ連携設定
    - LDAP 連携設定
    - Windows ドメイン連携設定
    - UPS 連携設定
    - SNMP マネージャ連携設定
6. 管理者設定
7. 証明書設定
8. DHCP 設定
9. クライアント設定
10. ネットワーク機器設定
11. スケジュール設定
12. バックアップ設定
13. リストア
14. アップデート

4.6.1 サーバ設定

サーバ設定では IP アドレスやホスト名などネットワーク関連の設定および再起動、シャットダウンを行います。

→ 基本設定

iBAQS-FX の IP アドレス、サブネットマスク、ゲートウェイ、DNS などの設定を行います。
詳細については、「4.2 設置前の準備[8]」を参照してください。

→ 時刻設定

時刻設定を行います。

サーバ設定-時刻画面

サーバ設定<<時刻タブ>>画面の項目

番号	画面項目	説明
(1)	管理 PC	管理 PC の日時です。
(2)	入力	設定したい日時を入力します。
(3)	選択	管理 PC の日時か入力日時かを選択します。

➢ NTP サーバから日時を取得する場合は、サーバ設定の基本タブの方から設定することが可能です。

→　**再起動**

iBAQS-FX の再起動を行います。

[再起動]ボタンをクリックすると再起動します。

サーバ設定-再起動画面

→　**シャットダウン**

iBAQS-FX のシャットダウンを行います。

[シャットダウン]ボタンをクリックするとシャットダウンします。

サーバ設定-シャットダウン画面

4.6.2　冗長化設定

冗長化設定では冗長構成に必要な情報の設定を行います。

iBAQS-FX ではアクティブ-スタンバイ型の冗長構成をサポートします。アクティブ状態で動作している iBAQS-FX をプライマリ、スタンバイ状態で動作している iBAQS-FX をセカンダリと表現します。

共有が必要な設定、ログに関してはネットワーク経由で常時ミラーリングされ、リソースに異常が発生した場合にはプライマリ機がシャットダウンすることによりセカンダリ機にフェイルオーバーを行い、認証処理を続けます。リソースチェックは約 10 秒に 1 回行われ、異常発生時には約 5 秒に 1 回に行います。異常発生を 3 回連続で検出するとフェイルオーバーを行います。

iBAQS-FX を 1 台で使用する際には設定不要です。

冗長化を構成する場合には 2 台のサーバの IP アドレス等の設定を終えてからプライマリとなるサーバ側から冗長化の設定を有効にしてください。セカンダリとなるサーバの設定はプライマリ側から自動的に行われますのでセカンダリとなるサーバでの設定は不要です。冗長化を設定する際にサーバの再起動やシャットダウン操作は不要です。

冗長構成で運用する場合にはネットワーク機器の RADIUS サーバ、DHCP リレーエージェントの参照先として仮想 IP アドレスを設定します。

※DHCP リレーエージェントによっては双方のサーバの実 IP アドレスを指定しなければならない場合があります。

冗長化設定画面

冗長化設定画面の項目

番号	画面項目	説明
(1)	冗長化	冗長化を行うか設定します。
(2)	通信インターフェース	ピアサーバと同期をとる際に利用するインターフェースです。サーバ設定の使用 LAN インターフェースと異なるインターフェースを指定することをおすすめします。
(3)	ピアサーバ IP アドレス	冗長化を構成するピアサーバの IP アドレスです。
(4)	仮想 IP アドレス	冗長構成時の仮想 IP アドレスです。 障害発生時にプライマリ機やセカンダリ機を意識することなく利用することのできる IP アドレスです。
(5)	再構成方式	冗長化の再構成方式です。 両サーバの起動順により自動で再構成を行うか、手動で再構成を行うかを選択します。

- 再構成方式で「手動」を選択した場合、サーバの起動順により冗長化状態が「手動復旧待ち」の状態になる可能性があります。通常、サーバのシャットダウン・起動を行う順番としては、①セカンダリ機シャットダウン　②プライマリ機シャットダウン　③プライマリ機起動　④セカンダリ機起動　となります。「自動」を選択した場合は、起動順に関わらずにデータの新しいサーバをプライマリ機として再構成します。

冗長化設定確認画面

- 設定が完了するまでに、少々時間がかかります。
- 設定完了後に「強制同期中」(約 5 分から 10 分程度) となります。トップ画面で確認することができます。強制同期中には、サーバの再起動およびシャットダウンをすることができません。処理が終了するまでお待ちください。

4.6.3 システム設定

システム設定では iBAQS-FX の動作に関連する設定を行います。ここでは、認証モード/検知モード/MAC 収集モードの中からモードを選択します。通常のモードは認証モードで登録したクライアントのみ認証が成功します。検知モードは未登録のクライアントでも認証が成功しますが、未登録のクライアントの場合は不正アクセス状況画面に記録し、管理者にアラートメールが送信されます。(※1) MAC 収集モードは検知モードと同様に未登録のクライアントでも認証が成功し、アクセスした MAC アドレスや PC 名の情報を収集します。その他、ログ保持期間やアラートメールの送信有無の設定を行います。

※1…事前に管理者設定を行っておく必要があります。

→ モードの切り替え

システム設定-モード画面

システム設定-モード画面の項目

番号	画面項目	説明
(1)	ＭＡＣ収集モード	MAC アドレスを収集します。 MAC ベース認証の認証要求に対して全て認証成功を応答し、認証要求に使用された MAC アドレスを収集します。 また、PC 名を収集するために DHCP 機能を利用します。DHCP 機能が有効の場合には、各セグメントの DHCP モードはダイナミック割当として十分な払い出し範囲を設定して収集します。DHCP 機能が無効の場合には外部 DHCP へのリクエスト要求を参照し収集します。その際、外部 DHCP と別セグメントの場合にはルータやL3 スイッチにおいて DHCP リレー設定を行ってください。 実運用中に MAC 収集モードを有効にすると IEEE 802.1X 認証が正しく動作しなくなるのでご注意ください。
(2)	検知モード	未登録のクライアントでも認証が成功し、ネットワークに参加することができます。検知モードでは未登録クライアントからの接続を検知し、管理者にアラートメールでお知らせします。
(3)	認証モード	通常のモードで登録したクライアントのみ認証が成功し、ネットワークに参加することができます。認証モードでは未登録のクライアントは認証が失敗し、不正アクセスとして検出され、ネットワークへの参加が拒否されます。

- モードの使い分けとして、「MAC 収集モード」は、運用期間に入る前に MAC アドレスを収集する期間を設け、動作させます。その後、収集した情報をクライアント登録し、「検知モード」に変更します。検知モードでは、クライアント登録に漏れがある場合、アラートメールで通知されます。漏れがあった場合、再度クライアント登録を行います。クライアント登録が完了と判断できた後、「認証モード」に切り替えて、運用開始します。

→ 基本

システム設定−基本画面

システム設定−基本画面の項目

番号	画面項目	説明
(1)	ログ保持期間	サーバ内にログを蓄積する日数を設定します。0 日から 365 日まで指定可能で、デフォルトは 90 日です。設定日数を越えるログが削除対象となるため、0 日を指定してもログ削除処理実行当日分は削除されません。
(2)	パスワード生成桁数	パスワード入力項目欄に用意されている生成ボタンをクリックした際に作成するパスワードの桁数を設定します。
(3)	ワンタイムパスワード許容誤差	ワンタイムパスワードの生成誤差をステップ単位で設定します。トークンと iBAQS-FX 間で初期設定以降に時差が生じた場合や入力から認証に移るまでに時間を要した場合に許容するステップ数を設定してください。
(4)	パスワードロック	クライアントがユーザーID による認証を行う場合でかつパスワードの有効期限を設定した場合に指定した日数を経過したクライアントのパスワードをロックします。パスワードがロックされると該当クライアントは認証に失敗しますのでご注意ください。判定はクライアント状態監視処理にて行われます。
(5)	連続認証失敗ロック	クライアントが指定した回数、連続で認証失敗となった場合に

		クライアントの認証をロックします。認証がロックされると該当クライアントは認証に失敗しますのでご注意ください。指定した回数に達する前に認証成功となった場合、連続失敗回数はリセットされます。
(6)	事前登録 使用	事前登録を行うか設定します。 事前登録を行う場合、次の URL から事前登録を行うことが可能になります。 http://<iBAQS-FX の IP アドレス>:10080/entry.jsp 事前登録された情報は、「事前登録状況」画面に表示されます。事前登録情報を承認許可することでクライアント登録されます。
(7)	事前登録 IP アドレス	事前登録で IP アドレスの指定を行うか設定します。 指定しないを設定した場合は、アクセスしている通信機器の IP アドレスは表示されますが登録はされません。

→ メール

システム設定-メール画面

システム設定-基本画面の項目

番号	画面項目	説明
(1)	差出人メールアドレス	差出人メールアドレスです。
(2)	SNMP サーバ	SNMP サーバです。 IPv4 アドレスまたは FQDN で設定します。
(3)	メール認証 利用	メール認証の利用を設定します。 「なし」／「SNMP 認証」／「POP before SNMP 認証」から選択します。
(4)	メール認証 ユーザーID	メール認証で利用するユーザーID です。

(5)	メール認証 パスワード	メール認証で利用するパスワードです。
(6)	メール認証 POP サーバ	POP before SNMP 認証時に利用する POP サーバです。
(7)	アラートメール 不正アクセス検出時	未登録クライアントのネットワーク接続を検出した際にアラートメールを送信します。指定した間隔の間に同一クライアントからの不正アクセスが発生した場合には再送を行いません。再送間隔の設定は 0 分から 99 分まで設定できます。デフォルトは 5 分です。0 を指定した場合には検出の都度アラートメールを送信します。
(8)	アラートメール 冗長化運転切替時	冗長構成中に運転状態が切り替わった際にアラートメールを送信します。運転状態は、通常運転／縮退運転／手動復旧待ち／異常があります。
(9)	アラートメール アップデート有の場合	アップデート確認処理実行時に新規アップデートを検出するとアラートメールを送信します。
(10)	アラートメール 一定期間認証なしの場合	クライアント状態監視処理実行時に指定された日数で認証が行われていないクライアントを検出した際にアラートメールを送信します。
(11)	アラートメール 認証有効期限切れ	クライアント状態監視処理実行時に指定された日数で認証有効期限の切れるクライアントを検出するとアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 7 日です。
(12)	アラートメール パスワード期限切れ（管理者）	クライアント状態監視処理実行時に指定された日数でパスワード有効期限の切れるクライアントを検出すると管理者宛にアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 3 日です。
(13)	アラートメール パスワード期限切れ（利用者）	クライアント状態監視処理実行時に指定された日数でパスワード有効期限の切れるクライアントを検出すると利用者宛にアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日から 99 日まで設定できます。デフォルトは 7 日です。クライアント設定でメールアドレスが入力されていない場合には送信されません。
(14)	アラートメール 認証局／証明書期限切れ	クライアント状態監視処理実行時に指定された日数で認証局/証明書の有効期限切れを検出するとアラートメールを送信します。送信は該当した場合に 1 回のみ行われます。日数は 0 日

		から 99 日まで設定できます。デフォルトは 7 日です。
(15)	アラートメール 未登録ネットワーク機器 認証通知	未登録のネットワーク機器で認証が行われた際にアラートメールを送信します。
(16)	アラートメール 事前登録時	事前登録が行われた場合にアラートメールを送信します。
(17)	アラートメール システム異常時	システムの異常を検出するとアラートメールを送信します。

- メール認証のパスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

→ **集中管理**

複数拠点に配置されている iBAQS-FX(子機)を 1 台の iBAQS-FX(親機)で集中管理します。子機の登録可能台数は、100 台です。子機を 1 台登録することで自動的に集中管理が開始されます。子機の状態は、「集中管理状況」画面で確認することができます。

システム設定-集中管理画面

システム設定-集中管理画面の項目

番号	画面項目	説明
(1)	現在の集中管理状態	現在の集中管理状態です。 集中管理なし：集中管理していません 親機：親機として集中管理しています 子機：子機として集中管理されています
(2)	追加ボタン	子機を追加します。 子機追加画面がポップアップ表示されます。
(3)	IP アドレス	子機の IP アドレスです。
(4)	設置場所	子機の設置場所です。

➢ 子機をクリックすることで、子機編集画面がポップアップ表示されます。

子機追加画面

子機追加画面の項目

番号	画面項目	説明
(1)	IP アドレス	子機の IP アドレスです。
(2)	設置場所	子機の設置場所です。

子機編集画面

子機編集画面の項目

番号	画面項目	説明
(1)	IP アドレス	子機の IP アドレスです。
(2)	設置場所	子機の設置場所です。

4.6.4 ライセンス設定

ライセンス設定では登録されているライセンスキー、ライセンス数、ライセンス有効期限を確認、更新することができます。オフラインでもライセンス情報を更新することができます。

→ ライセンス有効期限の確認

iBAQS-FX のライセンス有効期限の確認および更新を行います。
ライセンス有効期限延長の手続きを行った際に、ご利用ください。

ライセンス設定画面

→ ライセンス設定

ライセンス設定詳細ついては、「4.4 ライセンスキーを登録」を参照ください。

4.6.5 外部連携設定

外部連携設定では、外部機器との連携設定を行います。

外部連携設定画面

外部連携設定画面の項目

番号	画面項目	説明
(1)	syslog サーバ	syslog サーバと連携します。
(2)	LDAP	LDAP サーバと連携します。
(3)	Windows ドメイン	Windows ドメインと連携します。
(4)	UPS	UPS と連携します。
(5)	SNMP マネージャ	SNMP マネージャと連携します。

➢ 項目をクリックすることで、各画面に遷移します。

4.6.6 syslog サーバ連携設定

syslog サーバ連携設定では、外部の syslog サーバに出力することができます。RADIUS と DHCP のログを外部の syslog サーバに出力することができます。

syslog サーバ連携設定画面

syslog サーバ連携設定画面の項目

番号	画面項目	説明
(1)	使用	使用するか設定します。
(2)	ホスト・ポート	syslog サーバのホスト名とポート番号です。
(3)	ファシリティ	syslog サーバへ出力する際のファシリティです。

4.6.7 LDAP 連携設定

LDAP 連携設定では、外部の LDAP サーバを利用して認証することができます。LDAP サーバは 4 つまで指定できます。評価の順番は LDAP1、LDAP2、LDAP3、LDAP4、ローカルとなります。ローカルでも認証できないものに関して認証失敗を応答します。

<u>**※LDAP 連携ではシンプルバインドを用いて LDAP サーバ側で認証を行うため、PAP での認証のみをサポートします。**</u>

LDAP 連携設定画面

LDAP 連携設定画面の項目

番号	画面項目	説明
(1)	使用	LDAP 連携を行うかどうかを設定します。
(2)	サーバ名	LDAP サーバのホスト名です。
(3)	ポート番号	LDAP サーバのポート番号です。通常 389、SSL 使用時 636 です。
(4)	SSL 使用	SSL 使用を行うかどうかを設定します。
(5)	管理者 DN	LDAP の管理者 DN を設定します。
(6)	管理者パスワード	LDAP の管理者パスワードを設定します。
(7)	検索ベース DN	LDAP の検索の基点となる DN を設定します。
(8)	検索対象属性	LDAP の検索対象となるアトリビュートを設定します。

➢ 管理者パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

4.6.8 Windows ドメイン連携設定

Windows ドメイン連携設定では、Windows ドメイン認証することができます。Windows ドメイン認証では、Windows ドメインサーバに登録されているユーザーID とパスワードを照合します。対象サーバは、Windows NT4 ベースのドメインサーバと Active Directory ドメインサーバです。

【Windows ドメイン認証するためには】

以下の設定を行う必要があります。

◆ クライアント

① サーバ証明書は、iBAQS-FX から認証局証明書の発行／ダウンロードし、信頼できる証明書としてインポートしてください。

② EAP-PEAP 認証の設定を行ってください。

◆ 認証スイッチ

① 認証スイッチの接続ポートを 802.1X 認証ポートに設定してください。

◆ iBAQS-FX

① Windows ドメイン連携設定を行ってください。

◆ Windows ドメインサーバ

① ユーザー情報を登録してください。

➢ 認証局証明書の発行／ダウンロード方法は、「認証局設定」をご参照ください。

➢ EAP-PEAP 認証の設定詳細は、各デバイスの取扱説明書をご参照ください。

➢ 認証スイッチの 802.1X 認証ポートの設定は、各スイッチの取扱説明書をご参照ください。

Windows ドメイン連携設定画面

Windows ドメイン連携設定画面の項目

番号	画面項目	説明
(1)	Windows ドメイン認証	Windows ドメイン認証するか設定します。
(2)	Active Directory 使用	Windows ドメインサーバとして Active Directory サーバを使用するか設定します。
(3)	Active Directory ホスト名	Active Directory サーバのホスト名です。 入力制限）半角英数字　255 文字以内
(4)	ドメイン名	ドメイン名です。 入力制限）半角英数字　255 文字以内
(5)	管理者 ID	管理者 ID です。 入力制限）半角英数字　20 文字以内
(6)	管理者パスワード	管理者パスワードです。

- 設定が正常に完了した場合、iBAQS-FX がドメインサーバに参加登録されます。
- 管理者 ID、管理者パスワードに設定可能な文字は半角英数字と記号(. @ _ -)です。

4.6.9 UPS 連携設定

UPS 連携設定では、UPS を利用して電源供給が停止してしまった場合、正常にシャットダウンすることができます。バッテリー運転を 60 秒続けるとシャットダウン処理を開始します。商用電源回復後の自動通電が必要な場合、ES シリーズ以外をご使用ください。また、冗長構成時には、1 台の UPS を共有することもできます。その場合、ピアサーバをシャットダウンして自サーバをシャットダウンします。

- iBAQS-FX との接続は USB のみをサポートします。
- UPS が接続されていない状態で UPS 連携を有効にすることは出来ません。

UPS 連携設定画面

UPS 連携設定画面の項目

番号	画面項目	説明
(1)	UPS 連携	UPS を利用するか設定します。
(2)	冗長化時の UPS 共有	冗長構成時に UPS 共有するか設定します。 冗長構成していない時には表示されません。

4.6.10 SNMP マネージャ連携設定

SNMP マネージャ連携設定では、SNMP エージェントの設定を行います。SNMP マネージャからの SNMP 要求に応答します。SNMP で取得可能な情報は別紙「SNMP マネージャ連携で取得可能な情報について」をご確認ください。

SNMP マネージャ連携設定画面

SNMP マネージャ連携設定画面の項目

番号	画面項目	説明
(1)	SNMP マネージャ連携	SNMP エージェントとして動作するか設定します。
(2)	コミュニティ名	SNMP マネージャが read 権限でアクセスするためのコミュニティ名です。
(3)	マネージャ IP アドレス	アクセス許可するマネージャです。
(4)	システム設置場所	システム設置場所です。
(5)	システム管理責任者	システム管理責任者です。

4.6.11 管理者設定

iBAQS-FX の管理画面を利用する管理者の設定を行います。アラートメールを受信するためにはシステム設定でメールサーバの設定、管理者設定で管理者メールアドレスの設定が必要です。また、管理画面へのアクセス制限も可能です。

- デフォルトは、管理者 ID「manager」、パスワード「friend」です。

管理者設定-基本画面

管理者設定-基本画面の項目

番号	画面項目	説明
(1)	管理者 ID	管理者 ID です。 入力制限）半角英数字　20 文字以内
(2)	管理者パスワード	管理者パスワードです。
(3)	管理者メールアドレス PC 用	PC 用の管理者メールアドレスです。 管理者宛のアラートメールが送信されます。
(4)	管理者メールアドレス 携帯電話用	携帯電話用の管理者メールアドレスです。 管理者宛のアラートメールが送信されます。

- 管理者パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

管理者設定-アクセス制御画面

管理者設定-基本画面の項目

番号	画面項目	説明
(1)	アクセス制御	アクセス制御するか設定します。IP アドレス、ネットワーク範囲でアクセスを制限します。
(2)	指定	アクセス制御方法を選択します。 「指定なし」／「IP アドレス」／「ネットワーク空間」から選択します。
(3)	IP アドレス	アクセス許可する IP アドレスです。
(4)	ネットワーク空間	アクセス許可するネットワーク空間です。

4.6.12 証明書設定

証明書設定では、認証局証明書の発行／ダウンロード、クライアント証明書の発行／停止／回復／失効／ダウンロード、サーバ証明書への署名／停止／回復／失効／ダウンロード、証明書かんたんインストールの設定を行います。iBAQS-FX で発行した証明書を外部利用する際には失効リストを下記 URL から http プロトコルにて取得するように利用する機器に設定してください。

```
http://<iBAQS-FX の IP アドレス>:10080/crl
```

証明書設定-認証局画面

証明書設定-認証局画面の項目

番号	画面項目	説明
(1)	認証局編集リンク	認証局編集画面へ遷移します。
(2)	ステータス	認証局証明書の設定状態です。
(3)	作成日時	認証局証明書の作成日時です。
(4)	認証局名	認証局名です。
(5)	国名	国名です。
(6)	都道府県名	都道府県名です。

(7)	市区町村名	市区町村名です。
(8)	組織名	組織名です。
(9)	部署名	部署名です。
(10)	署名アルゴリズム	署名アルゴリズムです。
(11)	有効期限	有効期限です。
(12)	DER 形式ダウンロード	X.509 DER 形式の認証局証明書をダウンロードします。 認証局証明書を発行している場合のみ有効です。
(13)	PEM 形式ダウンロード	X.509 PEM 形式の認証局証明書をダウンロードします。 認証局証明書を発行している場合のみ有効です。

証明書設定-クライアント証明書画面

証明書設定-クライアント証明書画面の項目

番号	画面項目	説明
(1)	発行／失効ボタン	クライアント証明書発行画面へ遷移します。
(2)	ダウンロードボタン	クライアント証明書ダウンロード画面へ遷移します。

証明書設定-サーバ証明書

証明書設定-サーバ証明書画面の項目

番号	画面項目	説明
(1)	サーバ証明書署名リンク	サーバ証明書署名のポップアップを表示します。
(2)	処理	サーバ証明書の停止、失効、削除を指定します。
(3)	処理ボタン	サーバ証明書の停止、失効、削除を行います。

証明書設定-サーバ証明書署名

証明書設定-サーバ証明書署名画面の項目

番号	画面項目	説明
(1)	証明書署名要求	サーバ証明書を利用するデバイスで生成した証明書署名要求(PEM 形式)を入力します。
(2)	有効期間	有効期間です。 1 年／2 年／3 年／4 年／5 年／10 年／15 年／20 年　から選択

		します。
(3)	閉じるボタン	ポップアップウィンドウを閉じます。
(4)	署名ボタン	サーバ証明書へ署名します。

証明書設定-証明書かんたんインストール

証明書かんたんインストールではメール認証を利用したクライアント証明書のインストール支援機能を提供します。

証明書設定-証明書かんたんインストール画面の項目

番号	画面項目	説明
(1)	利用案内リンク	証明書かんたんインストール利用案内画面へ遷移します。 証明書かんたんインストールが有効の場合に表示されます。
(2)	証明書かんたん インストール使用	主にスマートフォン向けに証明書のインストール支援機能を使用するか設定します。

		利用の流れは、「5.7.4 証明書かんたんインストール利用申請」と「5.7.5 証明書かんたんインストール」を参照ください。
(3)	証明書かんたんインストール URL 有効期間	証明書かんたんインストール利用案内メールで通知される URL の有効期間を設定します。有効期限が切れた場合には再度案内メールの送付または申請手続きが必要です。
(4)	設定ナビ使用	スマートフォンの VPN 接続アプリケーション設定支援機能を使用するか設定します。 詳細は「5.7.6 設定ナビ」を参照ください。
(5)	設定ナビ 機器名	VPN 装置の種類を選択します。現在は Juniper SA(Junos Pulse iOS 版)のみサポートしています。
(6)	設定ナビ 接続名	VPN 接続アプリケーションに設定する接続名称を設定します。
(7)	設定ナビ 接続サーバ名	VPN 接続アプリケーションに設定する VPN 装置のサーバ（接続先)名です。 IPv4 アドレスまたは FQDN で設定します。

4.6.13 認証局設定

認証局設定では、認証局証明書の発行を行います。認証局を更新する場合、既に発行している認証局証明書やクライアント証明書は使用できなくなりますのでご注意ください。

認証局設定画面

認証局設定画面の項目

番号	画面項目	説明
(1)	認証局名	認証局名です。
(2)	国名	国名です。 JP（日本）固定です。
(3)	都道府県名	都道府県名です。
(4)	市区町村名	市区町村名です。
(5)	組織名	組織名です。
(6)	部署名	部署名です。
(7)	署名アルゴリズム	署名アルゴリズムです。 MD5 または SHA1 を選択します。
(8)	有効期限	有効期限です。 5 年／10 年／15 年／20 年／25 年 を選択します。

4.6.14 クライアント証明書発行

クライアント証明書発行では、クライアント証明書の発行／停止／回復／失効を行います。

クライアント証明書発行画面

クライアント証明書発行画面の項目

番号	画面項目	説明
(1)	検索ボタン	発行状態（指定なし／未発行／停止中／発行済）を検索条件として検索します。
(2)	利用者名	利用者名です。
(3)	PC 名	PC 名です。
(4)	ユーザーID	ユーザーID です。
(5)	状態	発行状態です。 未発行／停止中／発行済をアイコンで示します。
(6)	有効期限	証明書の有効期限を表示します。
(7)	処理	発行、停止、回復、失効の処理を選択します。
(8)	クライアント証明書処理ボタン	選択した処理の内容に従って発行、停止、回復、失効を行います。

4.6.15 クライアント証明書ダウンロード

クライアント証明書ダウンロードでは、発行済みのクライアント証明書をダウンロードします。

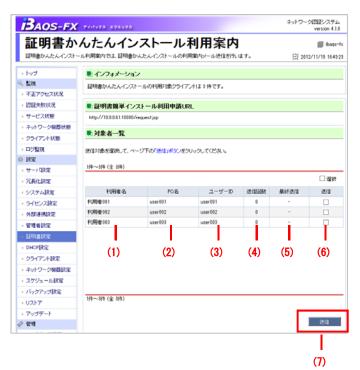
クライアント証明書ダウンロード画面

クライアント証明書ダウンロード画面の項目

番号	画面項目	説明
(1)	利用者名	利用者名です。
(2)	PC 名	PC 名です。
(3)	ユーザーID	ユーザーID です。
(4)	有効期限	クライアント証明書の有効期限です。
(5)	ダウンロードチェックボックス	ダウンロードするクライアント証明書をチェックします。
(6)	クライアント証明書ダウンロードボタン	チェックしたクライアント証明書をダウンロードします。 複数のクライアント証明書を一括ダウンロードできます。

4.6.16 証明書かんたんインストール利用案内

証明書かんたんインストール利用案内では、メールアドレスの登録されているクライアントに対して証明書かんたんインストールの利用案内メールを送信します。

証明書かんたんインストール利用案内画面

クライアント証明書ダウンロード画面の項目

番号	画面項目	説明
(1)	利用者名	利用者名です。
(2)	PC 名	PC 名です。
(3)	ユーザーID	ユーザーID です。
(4)	送信回数	メールを送信した回数です。
(5)	最終送信	最後にメールを送信した年月日です。
(6)	送信チェックボックス	メールを送信するクライアントをチェックします。
(7)	送信ボタン	チェックしたクライアントへメールを送信します。複数のクライアントへメールを一斉送信できます。

4.6.17 DHCP 設定

DHCP 設定では DHCP サーバの設定をします。基本タブは全セグメント共通の設定項目となります。DHCP 機能が有効な場合、セグメントタブの一番上に表示される iBAQS-FX の所属するセグメントはシステムの動作に必要なので削除できません。

DHCP 設定-基本画面

DHCP 設定-基本画面の項目

番号	画面項目	説明
(1)	DHCP 機能	DHCP 機能を有効にするか設定します。
(2)	リース時間	DHCP サーバがクライアントに払い出す IP アドレスのリース時間を設定します。セグメント毎にも設定可能で、セグメントに設定した値が優先されます。1 分から 6 日 23 時間 59 分まで設定できます。デフォルトは 1 日です。
(3)	DNS Primary	DNS Primary です。
(4)	DNS Secondary	DNS Secondary です。
(5)	DNS Tertiary	DNS Tertiary です。
(6)	DNS Suffix	DNS Suffix です。通常 1 つのみ指定します。Apple 社の iOS デバイスに限りスペース区切りで複数付与することが出来ます。
(7)	WINS Primary	WINS Primary です。
(8)	WINS Secondary	WINS Secondary です。
(9)	WINS Tertiary	WINS Tertiary です。

DHCP 設定-セグメント画面

DHCP 設定-セグメント画面の項目

番号	画面項目	説明
(1)	セグメント追加リンク	セグメント追加画面へ遷移します。
(2)	セグメント名	セグメント名です。
(3)	モード	DHCP モードです。 固定／ダイナミック／特定のいずれかです。
(4)	ネットワーク	セグメントのネットワークアドレスです。
(5)	サブネット	セグメントのサブネットマスクです。
(6)	ゲートウェイ	セグメントのゲートウェイアドレスです。

➢ 項目をクリックすると、「セグメント編集画面」へ遷移します。

4.6.18 セグメント追加

セグメント追加では、DHCP サーバで扱うネットワークの追加を行います。

セグメント追加画面

セグメント追加画面の項目

番号	画面項目	説明
(1)	セグメント名	セグメント名です。 入力制限）30 文字以内　全角文字使用可）
(2)	ネットワークアドレス	ネットワークアドレスです。
(3)	サブネットマスク	サブネットマスクです。
(4)	デフォルトゲートウェイ	デフォルトゲートウェイです。

(5)	DHCP モード	DHCP モードを選択します。 「固定割当」は、MAC アドレスに対応した IP アドレスを固定的に割り当てます。当セグメントに所属するクライアントは MAC アドレスと IP アドレスの入力が必須となります。 「ダイナミック割当」は、未知の MAC アドレスに対しても払い出し範囲から IP アドレスを割り当てます。当セグメントに所属していないクライアントに対しても IP アドレスを割り当てるため非認証ポートの存在するセグメントでの利用は注意が必要です。 「特定割当」は、既知の MAC アドレスに対してのみ払い出し範囲から IP アドレスを割り当てます。当セグメントに所属するクライアントは MAC アドレスの入力が必須となります。 ※特定割当は ver.4.0.1 以降、複数セグメントに設定できるようになりました。
(6)	払い出し範囲	IP アドレスの払い出し範囲の始点アドレス、終点アドレスを設定します。1 セグメントあたり 10 の払い出し範囲を設定することが可能です。DHCP モードがダイナミック割当、特定割当の場合に表示されます。
(7)	リース時間	リース時間です。セグメント単位で設定します。
(8)	DNS Primary	DNS Primary です。
(9)	DNS Secondary	DNS Secondary です。
(10)	DNS Tertiary	DNS Tertiary です。
(11)	DNS Suffix	DNS Suffix です。通常 1 つのみ指定します。Apple 社の iOS デバイスに限りスペース区切りで複数付与することが出来ます。
(12)	WINS Primary	WINS Primary です。
(13)	WINS Secondary	WINS Secondary です。
(14)	WINS Tertiary	WINS Tertiary です。

4.6.19 セグメント編集

セグメント編集では、セグメントの編集／削除を行います。

セグメント編集画面

セグメント編集画面の項目

番号	画面項目	説明
(1)	セグメント名	セグメント名です。 入力制限）30 文字以内　全角文字使用可）
(2)	ネットワークアドレス	ネットワークアドレスです。
(3)	サブネットマスク	サブネットマスクです。
(4)	デフォルトゲートウェイ	デフォルトゲートウェイです。

(5)	DHCP モード	DHCP モードを選択します。 「固定割当」は、MAC アドレスに対応した IP アドレスを固定的に割り当てます。当セグメントに所属するクライアントは MAC アドレスと IP アドレスの入力が必須となります。 「ダイナミック割当」は、未知の MAC アドレスに対しても払い出し範囲から IP アドレスを割り当てます。当セグメントに所属していないクライアントに対しても IP アドレスを割り当てるため非認証ポートの存在するセグメントでの利用は注意が必要です。 「特定割当」は、既知の MAC アドレスに対してのみ払い出し範囲から IP アドレスを割り当てます。当セグメントに所属するクライアントは MAC アドレスの入力が必須となります。 ※特定割当は ver.4.0.1 以降、複数セグメントに設定できるようになりました。
(6)	払い出し範囲	IP アドレスの払い出し範囲の始点アドレス、終点アドレスを設定します。1 セグメントあたり 10 の払い出し範囲を設定することが可能です。DHCP モードがダイナミック割当、特定割当の場合に表示されます。
(7)	リース時間	リース時間です。セグメント単位で設定します。
(8)	DNS Primary	DNS Primary です。
(9)	DNS Secondary	DNS Secondary です。
(10)	DNS Tertiary	DNS Tertiary です。
(11)	DNS Suffix	DNS Suffix です。通常 1 つのみ指定します。Apple 社の iOS デバイスに限りスペース区切りで複数付与することが出来ます。
(12)	WINS Primary	WINS Primary です。
(13)	WINS Secondary	WINS Secondary です。
(14)	WINS Tertiary	WINS Tertiary です。
(15)	削除ボタン	セグメントを削除します。
(16)	編集ボタン	セグメントを編集します。

4.6.20 クライアント設定

クライアント設定では、認証を行うクライアントの設定を行います。

クライアント設定画面

クライアント設定画面の項目

番号	画面項目	説明
(1)	検索ボタン	以下の検索条件を利用して絞り込み検索できます。 →　ソート項目：利用者名／PC 名／MAC アドレス-降順／昇順 →　検索文字列（利用者名／PC 名対象） →　セグメント名
(2)	OTP 利用案内へ	ワンタイムパスワード利用案内画面へ遷移します。 認証パターンがワンタイムパスワード認証またはワンタイムパスワード ＆ MAC アドレス認証でトークン種別がソフトウェア(30 秒)、メールアドレスが設定されているクライアントが存在する場合に表示されます。
(2)	新規追加へリンク	クライアント追加画面へ遷移します。
(3)	CSV 一括変更リンク	クライアント一括変更画面へ遷移します。
(4)	一括削除リンク	クライアント一括削除画面へ遷移します。
(5)	利用者名	利用者名です。
(6)	PC 名	PC 名です。
(7)	MAC アドレス	MAC アドレスです。
(8)	セグメント名	所属するセグメント名です。
(9)	IP アドレス	IP アドレスです。

- 項目をクリックすると、「クライアント編集画面」へ遷移します。

4.6.21 クライアント追加

クライアント追加では、認証を行うクライアントを追加します。IP アドレスを固定割当する場合のみ DHCP タブで IP アドレスを設定してください。

※認証の項目は選択する認証パターンに応じて表示します。

クライアント追加-基本画面

クライアント追加-基本画面の項目

番号	画面項目	説明
(1)	利用者名	利用者名です。
(2)	PC 名	PC 名です。
(3)	認証パターン	認証パターンを選択します。 ① MAC アドレス認証 ② ユーザーID 認証 ③ クライアント証明書認証 ④ ユーザーID ＆ MAC アドレス認証 ⑤ クライアント証明書 & MAC アドレス認証 ⑥ ワンタイムパスワード認証 ⑦ ワンタイムパスワード & MAC アドレス認証
(4)	MAC アドレス	MAC アドレスです。MAC アドレスを利用した認証を行う場合に入力が必要です。また、DHCP モードが固定、特定のセグメントに所属させる場合にも入力が必要です。
(5)	ユーザーID	ユーザーID です。ユーザーID 認証、クライアント証明書認証、ワンタイムパスワード認証を行う場合に入力が必要です。
(6)	パスワード	パスワードです。ユーザーID 認証、クライアント証明書認証を行う場合に入力が必要です。
(7)	クライアント証明書有効期限	クライアント証明書の有効期限を選択します。 1 年／2 年／3 年／4 年／5 年／10 年／15 年／20 年
(8)	トークンタイプ	トークンの種類を選択します。 ハードウェア(60 秒)…ハードウェアトークンでタイムステップが 60 秒の製品(飛天ジャパン製 C200 など) ハードウェア(30 秒)…ハードウェアトークンでタイムステップが 30 秒の製品 ソフトウェア(30 秒)…ソフトウェアトークンでタイムステップが 30 秒の製品(OATH Token や Android Token など)
(9)	トークンパスワード 生成桁数	トークンが生成するワンタイムパスワードの桁数です。 トークンの設定値に応じて 6～8 の範囲で設定します。 ハードウェアトークンの標準品は 6 桁、ソフトウェアトークンの既定値は 6 桁です。
(10)	トークン乱数キー	トークンがワンタイムパスワードを生成する際に使用する乱数キー(シード)です。40 桁の 16 進数で設定します。 ハードウェアトークンの場合はトークン購入時にメーカーから提供される情報を入力します。ソフトウェアトークンの場合

		はトークン側と同一の値を入力します。メールアドレスを入力することで、利用案内メールを送信することも可能です。
(11)	トークン誤差	トークンの時計と iBAQS-FX の時計の差です。 ステップ数で設定し、-50 から 50 の範囲で設定します。 タイムステップが 60 秒の場合には 50 分、タイムステップが 30 秒の場合には 25 分までの差を調整可能です。 トークンタイプ、トークンパスワード生成桁数、トークン乱数キーを入力した上でトークンの生成するワンタイムパスワードをワンタイムパスワード欄に入力し、「誤差検出」ボタンをクリックする事で自動的に検出を行います。
(12)	プロファイル	クライアントに適用するプロファイルを選択します。 プロファイルを適用することで認証スイッチの限定や任意のアトリビュートを認証スイッチに応答する事が可能になります。
(13)	クライアント利用	クライアント利用するか設定します。クライアントの一時利用停止を行いたい場合に「しない」に設定します。クライアント証明書を利用するクライアントでは証明書の失効を伴わずにネットワーク接続を禁止することができます。即時反映されます。
(14)	認証有効期限制御	認証有効期限制御を行います。 有効期限が切れるとクライアント状態監視処理によりネットワーク接続が禁止されます。
(15)	VLAN 制御	ダイナミック VLAN で VLAN ID を付与します。
(16)	メールアドレス	メールアドレスです。
(17)	備考	備考です。

- 認証パターンの④と⑤と⑦は、組み合わせ認証です。論理積（AND）条件で認証成功となります。
- ユーザーID、パスワードに設定可能な文字は半角英数字と記号(. @ _ -)です。

クライアント追加-DHCP 画面

クライアント追加-基本画面の項目

番号	画面項目	説明
(1)	セグメント名	セグメント名です。 固定割当または特定割当のセグメントを選択してください。
(2)	IP アドレス	固定で割り振る IP アドレスです。 選択したセグメントのネットワーク範囲内で指定してください。 特定割当の場合には IP アドレスを入力しても払い出し範囲からの割当になります。

➢ 固定で IP アドレスを割り振らない場合は、設定する必要はありません。

4.6.22 クライアント編集

クライアント編集では、認証を行うクライアントを編集します。

※認証の項目は選択する認証パターンに応じて表示します。

クライアント編集-基本画面

クライアント追加-基本画面の項目

番号	画面項目	説明
(1)	利用者名	利用者名です。
(2)	PC 名	PC 名です。
(3)	認証パターン	認証パターンを選択します。 ① MAC アドレス認証

		②　ユーザーID 認証 ③　クライアント証明書認証 ④　ユーザーID ＆ MAC アドレス認証 ⑤　クライアント証明書 & MAC アドレス認証
(4)	MAC アドレス	MAC アドレスです。MAC アドレスを利用した認証を行う場合に入力が必要です。また、DHCP モードが固定、特定のセグメントに所属させる場合にも入力が必要です。
(5)	ユーザーID	ユーザーID です。ユーザーID 認証、クライアント証明書認証、ワンタイムパスワード認証を行う場合に入力が必要です。
(6)	パスワード	パスワードです。ユーザーID 認証、クライアント証明書認証を行う場合に入力が必要です。
(7)	クライアント証明書有効期限	クライアント証明書の有効期限を選択します。 1 年／2 年／3 年／4 年／5 年／10 年／15 年／20 年
(8)	トークンタイプ	トークンの種類を選択します。 ハードウェア(60 秒)…ハードウェアトークンでタイムステップが 60 秒の製品(飛天ジャパン製 C200 など) ハードウェア(30 秒)…ハードウェアトークンでタイムステップが 30 秒の製品 ソフトウェア(30 秒)…ソフトウェアトークンでタイムステップが 30 秒の製品(OATH Token、Android Token など)
(9)	トークンパスワード生成桁数	トークンが生成するワンタイムパスワードの桁数です。 トークンの設定値に応じて 6～8 の範囲で設定します。 ハードウェアトークンの標準品は 6 桁、ソフトウェアトークンの既定値は 6 桁です。
(10)	トークン乱数キー	トークンがワンタイムパスワードを生成する際に使用する乱数キー(シード)です。40 桁の 16 進数で設定します。 ハードウェアトークンの場合はトークン購入時にメーカーから提供される情報を入力します。ソフトウェアトークンの場合はトークン側と同一の値を入力します。メールアドレスを入力することで、利用案内メールを送信することも可能です。
(11)	トークン誤差	トークンの時計と iBAQS-FX の時計の差です。 ステップ数で設定し、-50 から 50 の範囲で設定します。 タイムステップが 60 秒の場合には 50 分、タイムステップが 30 秒の場合には 25 分までの差を調整可能です。 トークンタイプ、トークンパスワード生成桁数、トークン乱数キーを入力した上でトークンの生成するワンタイムパスワー

		ドをワンタイムパスワード欄に入力し、「誤差検出」ボタンをクリックする事で自動的に検出を行います。
(12)	プロファイル	クライアントに適用するプロファイルを選択します。 プロファイルを適用することで認証スイッチの限定や任意のアトリビュートを認証スイッチに応答する事が可能になります。
(13)	クライアント利用	クライアント利用するか設定します。クライアントの一時利用停止を行いたい場合に「しない」に設定します。クライアント証明書を利用するクライアントでは証明書の失効を伴わずにネットワーク接続を禁止することができます。即時反映されます。
(14)	認証有効期限制御	認証有効期限制御を行います。 有効期限が切れるとクライアント状態監視処理によりネットワーク接続が禁止されます。
(15)	VLAN 制御	ダイナミック VLAN で VLAN ID を付与します。
(16)	メールアドレス	メールアドレスです。
(17)	備考	備考です。
(18)	パスワード更新日	パスワード更新日です。
(19)	登録日	登録日です。
(20)	削除ボタン	クライアントを削除します。
(21)	編集ボタン	クライアントを編集します。

- 認証パターンの④と⑤と⑦は、組み合わせ認証です。論理積（AND）条件で認証成功となります。
- ユーザーID、パスワードに設定可能な文字は半角英数字と記号(. @ _ -)です。

クライアント編集-DHCP 画面

クライアント編集-基本画面の項目

番号	画面項目	説明
(1)	セグメント名	セグメント名です。 固定割当または特定割当のセグメントを選択してください。
(2)	IP アドレス	固定で割り振る IP アドレスです。 選択したセグメントのネットワーク範囲内で指定してください。 特定割当の場合には IP アドレスを入力しても払い出し範囲からの割当になります。

- 固定で IP アドレスを割り振らない場合は、設定する必要はありません。

4.6.23 クライアント一括変更

クライアント一括変更では、CSV ファイルを用いたクライアントの一括登録、一括変更、一括削除を行うことができます。また、現在登録されているクライアントを一括変更で使用する形式の CSV ファイルでダウンロードできます。

クライアント一括変更画面

クライアント一括変更画面の項目

番号	画面項目	説明
(1)	インポートボタン	クライアント CSV ファイルを指定して、クライアントの一括変更を行います。
(2)	エクスポートボタン	登録されているクライアント情報を CSV ファイルでダウンロードします。

➢ CSV ファイルの形式については、当画面の「CSV ファイルの形式について」リンクから確認することができます。

4.6.24 クライアント一括削除

クライアント一括削除では、登録されているすべてのクライアントを一度に削除します。念のためにバックアップを採取してから削除されることを推奨します。クライアント証明書が発行済のクライアントがある場合、一括削除は利用できません。事前に発行済のクライアント証明書をすべて失効してください。

クライアント一括削除画面

クライアント追加-基本画面の項目

番号	画面項目	説明
(1)	はいボタン	クライアントを一括削除します。

4.6.25 ワンタイムパスワード利用案内

ワンタイムパスワード利用案内では、メールアドレスの登録されているソフトウェアトークン利用クライアントに対して設定内容を確認できる URL をメールで送信します。

ワンタイムパスワード利用案内画面

クライアント証明書ダウンロード画面の項目

番号	画面項目	説明
(1)	利用者名	利用者名です。
(2)	PC 名	PC 名です。
(3)	ユーザーID	ユーザーID です。
(4)	送信チェックボックス	メールを送信するクライアントをチェックします。
(5)	送信ボタン	チェックしたクライアントへメールを送信します。複数のクライアントへメールを一斉送信できます。

4.6.26 ネットワーク機器設定

ネットワーク機器設定では、認証スイッチの設定を行います。認証スイッチとして利用する場合には、設定が必要です。

ネットワーク機器設定画面

クライアント追加-基本画面の項目

番号	画面項目	説明
(1)	新規追加へリンク	ネットワーク機器追加画面へ遷移します。
(2)	CSV 一括変更リンク	ネットワーク機器一括変更画面へ遷移します。
(3)	一括削除リンク	ネットワーク機器一括削除画面へ遷移します。
(4)	機器名	機器名です。
(5)	機器 IP アドレス	機器 IP アドレスです。
(6)	設置場所	設置場所です。

- 項目をクリックすると、「ネットワーク機器編集画面」へ遷移します。

4.6.27 ネットワーク機器追加

ネットワーク機器追加では、認証スイッチとしてネットワーク機器を追加します。

ネットワーク機器追加画面

ネットワーク機器追加画面の項目

番号	画面項目	説明
(1)	機器名	機器名です。 入力制限）半角英数字　32 文字以内
(2)	機器種別	機器種別を選択します。
(3)	機器 IP アドレス	機器 IP アドレスです。
(4)	共有パスワード	RADIUS 認証で使用する共有パスワードです。
(5)	設置場所	設置場所です。
(6)	購入日（西暦）	購入日です。

➢ 共有パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

4.6.28 ネットワーク機器編集

ネットワーク機器編集では、認証スイッチとしてネットワーク機器を編集／削除します。

ネットワーク機器編集画面

ネットワーク機器編集画面の項目

番号	画面項目	説明
(1)	機器名	機器名です。 入力制限）半角英数字　32 文字以内
(2)	機器種別	機器種別を選択します。
(3)	機器 IP アドレス	機器 IP アドレスです。
(4)	共有パスワード	RADIUS 認証で使用する共有パスワードです。
(5)	設置場所	設置場所です。
(6)	購入日（西暦）	購入日です。
(7)	削除ボタン	ネットワーク機器を削除します。
(8)	編集ボタン	ネットワーク機器を編集します。

➢ 削除する前に削除する認証スイッチにクライアントが接続していないことを確認してから削除してください。

➢ 共有パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

4.6.29 ネットワーク機器一括変更

ネットワーク機器一括変更では、CSV ファイルを用いたネットワーク機器の一括登録、一括変更、一括削除を行うことができます。また、現在登録されているネットワーク機器を一括変更で使用する形式の CSV ファイルでダウンロードできます。

ネットワーク機器一括変更画面

ネットワーク機器一括変更画面の項目

番号	画面項目	説明
(1)	インポートボタン	ネットワーク機器 CSV ファイルを指定して、ネットワーク機器の一括変更を行います。
(2)	エクスポートボタン	登録されているネットワーク機器情報を CSV ファイルでダウンロードします。

- CSV ファイルの形式については、当画面の「CSV ファイルの形式について」リンクから確認することができます。

4.6.30 ネットワーク機器一括削除

ネットワーク機器一括削除では、登録されているすべてのネットワーク機器を一度に削除します。念のためにバックアップを採取してから削除されることを推奨します。

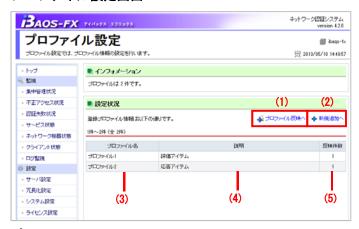
ネットワーク機器一括削除画面

ネットワーク機器一括削除画面の項目

番号	画面項目	説明
(1)	はいボタン	ネットワーク機器を一括削除します。

4.6.31 プロファイル設定

プロファイル設定では、クライアントに適用するプロファイルの設定を行います。たとえば評価アイテムを用いる事でユーザー認証を行う際、適用プロファイルに応じて利用可能な端末を制限したり認証可能なスイッチを限定する事が可能です。

プロファイル設定画面

プロファイル設定画面の項目

番号	画面項目	説明
(1)	プロファイル反映へ	プロファイル反映画面へ遷移します。
(2)	新規追加へ	プロファイル追加画面へ遷移します。
(3)	プロファイル名	プロファイル名です。
(3)	説明	プロファイルの説明です。
(4)	反映件数	プロファイルを適用しているクライアントの件数です。

- 項目をクリックすると、「プロファイル編集画面」へ遷移します。

4.6.32 プロファイル追加

プロファイル追加では、プロファイル情報の登録を行います。

プロファイル追加画面

プロファイル追加画面の項目

番号	画面項目	説明
(1)	プロファイル名	プロファイル名です。
(2)	説明	プロファイルの説明です。
(3)	任意の評価アイテム	評価に使用するアトリビュート、オペレーター、値を設定します。アトリビュートはリストボックスに候補が無い場合、入力する事も可能です。 ※入力値の方が優先されます。 ※複数の評価アイテムを設定すると論理積で評価されます。 ※複数のスイッチで接続を許可するような場合にはオペレーターで正規表現(=~)を利用してください。 例）192.168.1.2 もしくは 192.168.1.3 のスイッチの場合 →NAS-IP-Address=~192¥.168¥.1¥.2|192¥.168¥.1¥.3 例）192.168.1.10～192.168.1.99 のスイッチの場合 →NAS-IP-Address=~192¥.168¥.1¥.[1-9][0-9]

		※値は、1024 文字まで入力可能です。
(4)	任意の応答アイテム	スイッチに対して応答するアトリビュート、オペレーター、値を設定します。アトリビュートはリストボックスに候補が無い場合、入力する事も可能です。 ※入力値の方が優先されます。 ※応答可能な値は、248 文字までです。

4.6.33 プロファイル編集

プロファイル編集では、プロファイル情報の編集／削除を行います。

プロファイル編集画面

プロファイル編集画面の項目

番号	画面項目	説明
(1)	プロファイル名	プロファイル名です。
(2)	説明	プロファイルの説明です。
(3)	任意の評価アイテム	評価に使用するアトリビュート、オペレーター、値を設定します。アトリビュートはリストボックスに候補が無い場合、入力する事も可能です。

		※入力値の方が優先されます。 ※複数の評価アイテムを設定すると論理積で評価されます。 ※複数のスイッチで接続を許可するような場合にはオペレーターで正規表現(=~)を利用してください。 例）192.168.1.2 もしくは 192.168.1.3 のスイッチの場合 →NAS-IP-Address=~192¥.168¥.1¥.2|192¥.168¥.1¥.3 例）192.168.1.10～192.168.1.99 のスイッチの場合 →NAS-IP-Address=~192¥.168¥.1¥.[1-9][0-9] ※値は、1024 文字まで入力可能です。
(4)	任意の応答アイテム	スイッチに対して応答するアトリビュート、オペレーター、値を設定します。アトリビュートはリストボックスに候補が無い場合、入力する事も可能です。 ※入力値の方が優先されます。 ※応答可能な値は、248 文字までです。

4.6.34 プロファイル反映

プロファイル反映では、プロファイルをクライアントに一括適用します。

プロファイル反映画面

プロファイル反映画面の項目

番号	画面項目	説明
(1)	反映プロファイル	クライアントに適用するプロファイル名を選択します。
(2)	利用者名	クライアントの利用者名です。

(3)	PC 名	クライアントの PC 名です。
(4)	認証パターン	クライアントの認証パターンです。
(5)	現在のプロファイル	現在適用されているプロファイル名です。
(6)	対象チェックボックス	プロファイルを適用するクライアントをチェックします。
(7)	反映ボタン	チェックしたクライアントへ選択した反映プロファイルを適用します。複数のクライアントを一斉適用できます。

4.6.35 スケジュール設定

スケジュール設定では、定期的に処理を行うジョブのスケジューリングを行います。

スケジュール設定画面

スケジュール設定画面の項目

番号	画面項目	説明
(1)	ジョブ名	ジョブ名です。
(2)	状況	スケジュール状況です。
(3)	詳細	スケジュール詳細です。

➢ 項目をクリックすると、「スケジュール編集画面」へ遷移します。

4.6.36 スケジュール編集

スケジュール編集では、定期的に処理を行うジョブのスケジュールを編集します。

スケジュール編集画面

スケジュール編集画面の項目

番号	画面項目	説明
(1)	自動実行	自動実行するか設定します。
(2)	実行周期	実行周期を設定します。 実行周期はジョブにより異なります。
(3)	開始時刻	開始時刻です。

4.6.37 バックアップ設定

バックアップ設定では、設定情報のバックアップ方法を設定します。また、設定した内容での今すぐ(オンデマンド)バックアップ、ローカルバックアップファイルのダウンロードもできます。定期実行に関してはスケジュール設定のバックアップ処理で設定できます。

バックアップ設定-基本画面

バックアップ設定-基本画面の項目

番号	画面項目	説明
(1)	ローカル バックアップ	ローカルバックアップを実行するか設定します。
(2)	FTP バックアップ	FTP バックアップを実行するか設定します。
(3)	FTP サーバ IP アドレス	FTP サーバの IP アドレスです。
(4)	FTP ユーザーID	FTP のユーザーID です。
(5)	FTP パスワード	FTP のパスワードです。

(6)	FTP ファイル名（拡張子なし）	FTP へのバックアップファイル名です。実際に FTP サーバに PUT するファイルは[設定ファイル名].YYMMDD.tar.gz というファイル名になります。
(7)	Windows ファイル共有バックアップ	Windows ファイル共有のバックアップを実行するか設定します。
(8)	Windows ファイル共有サーバ IP アドレス	Windows ファイル共有のサーバ IP アドレスです。
(9)	Windows ファイル共有ユーザーID	Windows ファイル共有のユーザーID です。
(10)	Windows ファイル共有パスワード	Windows ファイル共有のパスワードです。
(11)	Windows ファイル共有共有名	Windows ファイル共有の共有名です。
(12)	Windows ファイル共有ファイル名（拡張子なし）	Windows ファイル共有のファイル名です。 共有リソースにコピーする際のファイル名を指定します。実際に共有リソースにコピーするファイルは[設定ファイル名].YYMMDD.tar.gz というファイル名になります。

- 各ユーザーID、パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

バックアップ設定-今すぐバックアップ画面

バックアップ設定-今すぐバックアップ画面の項目

番号	画面項目	説明
(1)	バックアップボタン	今すぐバックアップします。

バックアップ設定-ダウンロード画面

バックアップ設定-ダウンロード画面の項目

番号	画面項目	説明
(1)	ダウンロードボタン	ローカルバックアップファイルのダウンロードを行います。

4.6.38 リストア

リストアでは、バックアップファイルを用いた設定情報の復元を行います。また、初期設定へ戻すこともできます。リストア後は自動的に再起動が行われます。認証が停止しますので、運用中のリストアは行わないでください。

リストア画面

リストア画面の項目

番号	画面項目	説明
(1)	リストアボタン	指定したバックアップファイルを利用してリストアを行います。
(2)	工場出荷時に戻す	工場出荷時に戻します。

4.6.39 アップデート

アップデートでは、iBAQS-FX のアップデートの確認およびアップデートの適用を行います。オフラインでのアップデートも可能です。冗長構成を行っている場合は、冗長構成を解除する必要があります。

アップデート-オンライン画面

アップデート-オンライン画面の項目

番号	画面項目	説明
(1)	確認ボタン	アップデート確認を行います。 アップデートサーバへ接続し、アップデートの確認を行います。確認の結果はアップデート確認結果に表示します。アップデート確認では弊社のアップデートサーバへ http による通信を行います。iBAQS-FX をインターネットと直接通信できる場所に設置するかサーバ設定のプロキシサーバを設定してください。 アップデートがない場合には「現在、最新バージョンの状態です。アップデート情報はありません。」と表示します。
(2)	アップデートボタン	最新バージョンへアップデートします。 アップデートは回線状況により時間がかかる場合があります。ブラウザの戻るボタン等で画面を移動すると正常にアップデート処理が行われませんので再起動が行われるまでお待ちください。

- アップデート中にサーバの再起動やシャットダウンを行わないようにしてください。

アップデート-オフライン画面

アップデート-オフライン画面の項目

番号	画面項目	説明
(1)	アップデートボタン	オフラインアップデートファイルを用いて、アップデートを行います。

- オフラインでのアップデートをご希望の場合は、販売代理店までお問い合わせください。

- アップデート中にサーバの再起動やシャットダウンを行わないようにしてください。

以上で運用環境に応じた設定は完了です。

5　運用

iBAQS-FX の運用について説明します。

5.1　管理画面へのログイン

iBAQS-FX を利用したシステム運用では、iBAQS-FX の管理画面で行います。管理画面は、iBAQS-FX にネットワーク接続できるパソコンからブラウザでアクセスします。

5.1.1　ログイン

ログイン画面は以下の URL を指定して表示されます。

http://<iBAQS-FX の IP アドレス>:10080/

ログイン画面

- インストール直後は、管理者 ID「manager」、パスワード「friend」が設定されています。
- ログイン後にトップ画面が表示されます。

- 複数のパソコンから管理画面を操作することができます。
- セッションタイムアウト時間は、30 分です。「サーバ設定」にて変更可能です。

5.2 トップ

管理画面へのログインが成功するとトップ画面が表示されます。
トップ画面では、iBAQS-FX のシステム状況を表示します。

トップ画面

トップ画面の項目

番号	画面項目	説明
(1)	インフォメーション	システム全体の動作状況（正常／異常）です。
(2)	ライセンス有効期限	ライセンス有効期限です。 有効期限が切れた場合、アップデートが利用できなくなります。
	冗長化 （冗長構成時のみ表示）	冗長構成の状態です。 ➢ 通常運転中…正常に冗長構成で動作しています。 ➢ 縮退運転中…ピアサーバが存在しません。 ➢ 手動復旧待ち…ピアサーバと同期がとれていません。 ➢ 異常…ピアサーバとの接続に問題が発生しています。
	ミラーディスク （冗長構成時のみ表示）	ミラーディスクの状態です。 ➢ 通常同期中…正常にミラーリングを行っています。 ➢ 強制同期中(N%)…通常同期に加え、差分同期を行っています。
	集中管理状況 （集中管理中のみ表示）	集中管理状況です。 ➢ 正常動作中…子機が正常に動作しています。 ➢ 異常動作中…子機に異常が発生しています。
	モード	モードの設定状態です。 ➢ 認証モード…認証を行います。登録したクライアント情報と照合します。 ➢ 認証モード ＋ Windows ドメイン認証…認証モードと併用して Windows ドメイン認証を行います。 ➢ ＭＡＣ収集モード（DHCP 有効）…DHCP が有効で、MAC 収集を行います。認証はすべて成功します。 ➢ ＭＡＣ収集モード（DHCP 無効）…DHCP が無効で、MAC 収集を行います。認証はすべて成功します。 ➢ 検知モード…未登録クライアントを検知しアラートメールを送信します。認証はすべて成功します。
	ＭＡＣ収集状況 （ＭＡＣ収集モード時のみ表示）	ＭＡＣ収集状況です。 収集した件数を表示します。
	不正アクセス状況	不正アクセス状況です。 不正アクセスがあった場合、不正アクセス件数を表示します。
	認証失敗状況	認証失敗状況です。 認証失敗があった場合、認証失敗件数を表示します。

	サービス状態	サービス状態です。 ➢ 正常動作中…すべてのサービスが正常に動作しています。 ➢ 一部停止中…一部のサービスが停止しています。
	ネットワーク機器状態	ネットワーク機器状態です。 ➢ 正常動作中…すべてのネットワーク機器への通信が可能です。 ➢ 異常発生…ネットワーク機器への通信に異常が発生しています。
	クライアント登録数	クライアント登録数です。 ライセンス数までの登録が可能です。
	事前登録未承認数 （事前登録する場合のみ表示）	事前登録の未承認数です。 1 件以上登録されている場合は、「事前登録状況」画面で承認してください。

- ➢ 項目をクリックすると、各画面に遷移します。
- ➢ 強制同期中に認証が行えなくなることはありません。
- ➢ ピアサーバと強制同期が完了できない場合にはミラーディスクの物理的な破損の可能性があります。

- ➢ 冗長化「手動復旧待ち」の場合、再度冗長化設定を行ってください。
- ➢ 強制同期中にサーバの再起動やシャットダウンを行うことはできません。

5.3 監視

さまざまな角度からシステムを監視します。

5.3.1 集中管理状況

集中管理状況では、複数の拠点に配置されている iBAQS-FX（子機）のシステム状況を確認することができます。異常が発生した場合や、子機の詳細を確認したい場合は、項目をクリックすると子機のログイン画面へダイレクトアクセスします。当画面は、「システム設定」<<集中管理>>で集中管理を行った場合のみ表示されます。

集中管理状況画面

集中管理状況画面の項目

番号	画面項目	説明
(1)	確認日時	子機への確認を行った日時です。
(2)	確認ボタン	クリックすると、リアルタイムで子機の状態を取得します。
(3)	IP アドレス	子機の IP アドレスです。
(4)	運行	子機の運行状況です。 ➢ …正常に運行しています。 ➢ …異常が発生しています。
(5)	通信	子機への ping 状況です。 ➢ …正常に通信しています。 ➢ …通信に異常が発生しています。
(6)	不正アクセス	子機の不正アクセス状況です。 不正アクセス件数が表示されます。

(7)	サービス	子機のサービス状態です。 ➢ …正常に動作しています。 ➢ …一部のサービスに異常が発生しています。
(8)	NAS	子機のネットワーク機器状態です。 ➢ …正常に動作しています。 ➢ …一部のネットワーク機器に異常が発生しています。
(9)	クライアント	子機に登録されているクライアント件数です。
(10)	有効期限	子機のライセンス有効期限です。
(11)	設置場所	子機の設置場所です。

- 集中管理する場合のみ表示されます。
- 子機に異常が発生している場合には、項目をクリックして子機の管理画面にアクセスし、詳細を確認してください。
- 子機の管理画面にアクセスする際には子機の管理者 ID、パスワードが必要です。

5.3.2 事前登録状況

事前登録状況では、利用者から事前登録された状況を表示し、承認を行います。一括で承認許可したり個別で承認許可したりくることが可能です。承認を許可した場合は、自動でクライアント登録されます。承認を拒否した場合には、登録されません。当画面は、「システム設定」<<基本>>で事前登録を行う、と設定した場合のみ表示されます。

事前登録状況画面

事前登録状況画面の項目

番号	画面項目	説明
(1)	検索ボタン	ステータスを検索条件として検索します。
(2)	一括削除	事前登録を一括削除します。
(3)	一括許可	未承認、拒否を一括許可します。 一括許可された事前登録はクライアントに登録されます。
(4)	一括拒否	未承認、拒否を一括拒否します。
(5)	チェックボックス	一括許可する項目をチェックします。
(6)	認証	事前登録した認証パターンです。
(7)	利用者名	事前登録した利用者名です。
(8)	PC 名	事前登録した PC 名です。
(9)	IP アドレス	事前登録した IP アドレスです。
(10)	MAC アドレス	事前登録した MAC アドレスです。
(11)	申請日時	事前登録した申請日時です。
(12)	ステータス	事前登録のステータスです。 ➢ 未承認…承認待ちの状態です。 ➢ 許可…承認を許可した状態です。 ➢ 拒否…承認を拒否した状態です。 ➢ 登録済…クライアントが登録されている状態です。

- 事前登録する場合のみ表示されます。
- IP アドレスの登録について、DHCP 機能を有効にして固定 IP アドレスで運用される場合は、固定割当のセグメント内の IP アドレスを指定してください。ダイナミック割当のセグメント内の IP アドレスを指定した場合は、指定した IP アドレスは払い出されません。
- 項目をクリックすると「事前登録編集」画面に遷移します。

事前登録編集画面

事前登録編集画面の項目

番号	画面項目	説明
(1)	認証パターン	事前登録した認証パターンです。
(2)	利用者名	事前登録した利用者名です。
(3)	PC 名	事前登録した PC 名です。
(4)	IP アドレス	事前登録した IP アドレスです。
(5)	MAC アドレス	事前登録した MAC アドレスです。
(6)	ユーザーID	事前登録したユーザーID です。
(7)	メールアドレス	事前登録したメールアドレスです。
(8)	トークンパスワード生成桁数	事前登録したトークンパスワード生成桁数です。
(9)	トークン乱数キー	事前登録したトークン乱数キーです。
(10)	ステータス	事前登録のステータスです。希望の状態に変更可能です。 ➢ 未承認…承認待ちの状態です。 ➢ 許可…承認を許可した状態です。 ➢ 拒否…承認を拒否した状態です。
(11)	申請日時	事前登録した申請日時です。
(12)	削除ボタン	対象の事前登録情報を削除します。
(13)	編集ボタン	対象の事前登録情報を編集します。

5.3.3　ＭＡＣ収集状況

ＭＡＣ収集状況では、収集したＭＡＣアドレス状況を表示します。収集した情報を一括でクライアント可能な CSV ファイルにエクスポート可能です。当画面は、「システム設定」<<モード>>でＭＡＣ収集モードに切り替えた場合のみ表示されます。また、ＭＡＣ収集モード（DHCP 無効）では、収集した情報をクライアント情報に自動登録することも可能です。

ＭＡＣ収集状況画面

ＭＡＣ収集状況画面の項目

番号	画面項目	説明
(1)	検索ボタン	事前登録を検索条件として検索します。
(2)	自動登録ボタン	収集した情報をクライアントに自動登録します。MAC 収集モード（DHCP 無効）時、検索条件に「事前登録なし(-)」を選択して検索した場合に表示されます。その際、利用者名と PC 名は自動採番されます。 利用者名：USER_0000000001 PC 名：PC_0000000001
(3)	登録用エクスポートボタン	クライアントに一括登録可能な形式の CSV ファイルをダウンロードします。検索条件に「事前登録なし(-)」を選択して検索した場合に表示されます。
(4)	表示内容エクスポートボタン	表示内容形式の CSV ファイルをダウンロードします。
(5)	一括削除ボタン	収集した情報を一括削除します。
(6)	収集日時	収集日時です。
(7)	MAC アドレス	収集した MAC アドレスです。
(8)	メーカー名	MAC アドレスに対するメーカー名です。
(9)	PC 名	収集した PC 名です。

(10)	IP アドレス	収集した IP アドレスです。
(11)	機器 IP	収集したネットワーク機器 IP アドレスです。
(12)	ポート	収集したネットワーク機器のポート番号です。
(13)	事前登録	事前登録状況です。 ➢ 未承認…事前登録の承認待ちです。 ➢ 許可…事前登録の承認が許可された状態です。 ➢ 拒否…事前登録の承認が拒否された状態です。 ➢ 登録済…クライアントが登録されている状態です。

- MAC 収集モードの場合のみ表示されます。
- 事前登録がある場合、項目をクリックすると「事前登録状況」画面へ遷移します。

5.3.4 不正アクセス状況

不正アクセス状況では、不正アクセスがあった場合の詳細を表示します。未登録のクライアントから認証要求があった場合に不正アクセスとして検出されます。検出された不正アクセス情報を正規クライアントとして登録することも可能です。

不正アクセス状況画面

不正アクセス状況画面の項目

番号	画面項目	説明
(1)	検索ボタン	ソート条件、検出日付、状態により検索します。
(2)	登録用エクスポート	クライアントとして登録可能な形式の CSV ファイルをダウンロードします。
(3)	表示内容エクスポート	表示内容形式の CSV ファイルをダウンロードします。
(4)	検出日時	不正アクセスの検出日時です。
(5)	MAC アドレス	不正アクセスの MAC アドレスです。
(6)	メーカー名	不正アクセスのメーカー名です。
(7)	状態	不正アクセス状態です。 ➢ 未確認…未確認の状態です。 ➢ 登録済…クライアント登録済みの状態です。 ➢ 削除済…削除済みの状態です。
(8)	機器名	不正アクセスを検出したネットワーク機器名です。
(9)	設置場所	不正アクセスを検出したネットワーク機器の設置場所です。
(10)	機器 IP	不正アクセスを検出したネットワーク機器の IP アドレスです。
(11)	ポート	不正アクセスを検出したネットワーク機器のポート番号です。
(12)	削除リンク	不正アクセス情報を削除します。

➢ 不正アクセス情報をもとに原因を対処してください。

5.3.5 認証失敗状況

認証失敗状況では、認証失敗があった場合の詳細を表示します。登録済みのクライアントが認証失敗した場合に検出されます。

認証失敗状況画面

認証失敗状況画面の項目

番号	画面項目	説明
(1)	検出日時	認証失敗検出日時です。
(2)	利用者名	認証失敗した利用者名です。
(3)	PC 名	認証失敗した PC 名です。
(4)	機器名	認証失敗を検出したネットワーク機器名です。
(5)	機器 IP	認証失敗を検出したネットワーク機器の IP アドレスです。
(6)	ポート	認証失敗を検出したネットワーク機器のポート番号です。
(7)	削除リンク	認証失敗情報を削除します。

➢ 認証失敗情報をもとに状況を把握してください。

5.3.6 サービス状態

サービス状態では、サービスの稼働状況を表示します。サービスが停止している場合は起動することができます。冗長構成時にサービスが停止するとフェイルオーバーの原因となります。

サービス状態画面

サービス状態画面の項目

番号	画面項目	説明
(1)	データベース	データベースサービスです。
	LDAP	LDAP サービスです。
	ワンタイムパスワード	ワンタイムパスワードサービスです。
	RADIUS	RADIUS サービスです。
	認証成功サービス	認証成功時に動作するサービスです。MAC 収集モード時にはMAC アドレスを収集し、検知モード時にはアラートメールを送信します。
	不正アクセス検出サービス	認証失敗時に動作するサービスです。不正アクセスが検出された場合にはアラートメールを送信します。
	SYSLOG	外部 syslog に出力するサービスです。 syslog 連携を行う場合に利用します。
	DHCP	DHCP サービスです。 DHCP 機能を有効にした場合に利用します。
	NTP	NTP サービスです。 iBAQS-FX の時刻を NTP サーバに同期します。 NTP を有効にした場合に利用します。
	同期サービス	冗長構成時にミラーディスクを用意し、ピアサーバと常時同期します。

		冗長構成に利用します。
	冗長監視サービス	フェイルオーバー対象のリソースを監視します。 冗長構成に利用します。
	ホスト名取得サービス	ホスト名を取得するサービスです。 MAC 収集モード（DHCP 無効）の場合に利用します。
	UPS 制御サービス	UPS と通信を行い、連携を行うサービスです。 UPS 連携を行う場合に利用します。
	SNMP エージェントサービス	SNMP エージェントとして動作するサービスです。 SNMP マネージャ連携を行う場合に利用します。

- 冗長構成時のフェイルオーバー対象となるサービスは、「データベース」「LDAP」「RADIUS」「認証成功サービス」「不正アクセス検出サービス」「SYSLOG」「DHCP」「ホスト名取得サービス」です。

- サービスが一部停止中の場合は、正常な動作を行えない可能性があります。

5.3.7 ネットワーク機器状態

ネットワーク機器状態では、登録済みのネットワーク機器への通信状態を表示します。スケジュール設定のネットワーク機器監視処理に設定した間隔で定期的にネットワーク機器へ ping 確認を行った結果が表示されます。ping は 1 機器あたり 3 回、タイムアウト 1 秒で実施し、100%応答が得られなかった場合に異常として扱います。ただし、一定期間(ネットワーク機器監視処理に設定した間隔)確認対象機器からの認証要求がない場合、100%応答が得られない場合においても正常とみなします。VPN 経由の監視も可能ですが、セッションが常に張られていない場合には正しく状態の監視ができない場合があります。VPN 装置にセッション維持機能が搭載されている場合には利用をお願いします。

ネットワーク機器状態画面

(1) (2) (3) (4) (5)

ネットワーク機器状態画面の項目

番号	画面項目	説明
(1)	機器名	ネットワーク機器名です。
(2)	機器 IP アドレス	ネットワーク機器の IP アドレスです。
(3)	設置場所	ネットワーク機器の設置場所です。
(4)	状態	ネットワーク機器の通信状態です。 ➢ …通信が可能な状態です。 ➢ …通信ができない状態です。
(6)	詳細	ネットワーク機器の通信状態詳細です。

➢ 項目をクリックすると、ネットワーク機器編集画面へ遷移します。

5.3.8 クライアント状態

クライアント状態では、クライアントの認証対象および最終認証日時を確認できます。また、エクスポートも可能です。

クライアント状態画面

クライアント状態画面の項目

番号	画面項目	説明
(1)	検索ボタン	検索文字列（利用者名・PC 名対象)、認証日付、認証対象で検索します。
(2)	エクスポートボタン	表示内容形式の CSV ファイルをダウンロードします。
(3)	利用者名	利用者名です。
(4)	PC 名	PC 名です。
(5)	認証パターン	認証パターンです。
(6)	認証日時	認証日時です。

➢ 項目をクリックすると、ネットワーク機器編集画面へ遷移します。

5.3.9 ログ監視

ログ監視では、各種ログへのリンクおよびエクスポートを行います。

ログ監視画面

利用場所検索画面の項目

番号	画面項目	説明
(1)	認証ログ	認証ログ画面に遷移します。
	DHCP リースログ	DHCP リースログ画面に遷移します。
	管理ログ	管理ログ画面に遷移します。
(2)	認証統計	認証統計画面に遷移します。
	DHCP リース統計	DHCP リース統計画面に遷移します。

(3)	エクスポートボタン	ログファイル（認証ログ／DHCP リースログ／管理ログ）、対象日付のデータを CSV ファイルでダウンロードします。

➢ データ量により、多少時間がかかる場合があります。

5.3.10 認証ログ

認証ログでは、認証履歴を確認できます。

認証ログ画面

認証ログ画面の項目

番号	画面項目	説明
(1)	検索ボタン	検索モード、ソート、認証日付、検索文字列（ユーザーID・MAC アドレス・PC 名・機器 IP アドレス対象）、認証結果にて検索します。
(2)	認証日時	認証日時です。
(3)	結果	認証結果です。 ➢　成功…認証成功です。 ➢　失敗…認証失敗です。
(4)	ユーザーID	ユーザーID です。
(5)	MAC アドレス	MAC アドレスです。
(6)	PC 名	PC 名です。
(7)	機器 IP	認証を受けたネットワーク機器の IP アドレスです。
(8)	ポート	認証を受けたネットワーク機器のポート番号です。

5.3.11 DHCP リースログ

DHCP リースログでは、DHCP リースに関するログを確認できます。

DHCP リースログ画面

DHCP リースログ画面の項目

番号	画面項目	説明
(1)	検索ボタン	検索モード、ソート、リース日付、検索文字列（IP アドレス・PC 名・MAC アドレス対象）にて検索します。
(2)	リース日時	DHCP のリース日時です。
(3)	IP アドレス	払い出した IP アドレスです。
(4)	PC 名	DHCP 要求を行った PC 名です。
(5)	MAC アドレス	DHCP 要求を行った MAC アドレスです。

5.3.12 管理ログ

管理ログでは、システムに関するログを確認できます。

管理ログ画面

DHCP リースログ画面の項目

番号	画面項目	説明
(1)	検索ボタン	検索モード、ソート、日付にて検索します。
(2)	日時	日時です。
(3)	ログ内容	ログ内容です。

5.3.13 認証統計

認証統計では、過去の認証結果を折れ線グラフで表示します。直近の過去 7 日間と過去 6 ヶ月間の認証状況を確認することができます。

認証統計画面

認証統計画面の項目

番号	画面項目	説明
(1)	過去 7 日間グラフ	直近の過去 7 日間の認証結果数をグラフ表示したものです。
(2)	過去 6 か月間グラフ	直近の過去 6 か月間の認証結果数をグラフ表示したものです。

5.3.14 DHCP リース統計

DHCP リース統計では、DHCP にて払い出された IP アドレスのリース状況を払い出し範囲ごとに円グラフで表示します。

DHCP リース統計画面

DHCP リース統計画面の項目

番号	画面項目	説明
(1)	DHCP リース状況	セグメント名、払い出し範囲、上限数、リース数、リース可能数、リース状況割合を表示します。

5.4 設定

システムの設定を行います。

➢ **サーバ設定**

サーバやネットワークに関する設定を行うには、サーバ設定画面を使用します。

詳細は、「4.5.1 サーバ設定」を参照ください。

➢ **冗長化設定**

冗長化に関する設定を行うには、冗長化設定画面を使用します。

詳細は、「4.5.2 冗長化設定」を参照ください。

➢ **システム設定**

システムに関する設定を行うには、システム設定画面を使用します。

詳細は、「4.5.3 システム設定」を参照ください。

➢ **ライセンス設定**

ライセンスに関する設定を行うには、ライセンス設定画面を使用します。

詳細は、「4.5.4 ライセンス設定」を参照ください。

➢ **外部連携設定**

外部連携に関する設定を行うには、外部連携設定画面を使用します。

詳細は、「4.5.5 外部連携設定」を参照ください。

➢ **管理者設定**

管理者に関する設定を行うには、管理者設定画面を使用します。

詳細は、「4.5.10 管理者設定」を参照ください。

➢ **証明書設定**

証明書に関する設定を行うには、証明書設定画面を使用します。

詳細は、「4.5.11 証明書設定」を参照ください。

➢ **DHCP 設定**

DHCP に関する設定を行うには、DHCP 設定画面を使用します。

詳細は、「4.5.15 DHCP 設定」を参照ください。

- **クライアント設定**

クライアントに関する設定を行うには、クライアント設定画面を使用します。
詳細は、「4.5.18 クライアント設定」を参照ください。

- **ネットワーク機器設定**

ネットワーク機器に関する設定を行うには、ネットワーク機器設定画面を使用します。
詳細は、「4.5.23 ネットワーク機器設定」を参照ください。

- **スケジュール設定**

スケジュールに関する設定を行うには、スケジュール設定画面を使用します。
詳細は、「4.5.26 スケジュール設定」を参照ください。

- **バックアップ設定**

バックアップに関する設定を行うには、バックアップ設定画面を使用します。
詳細は、「4.5.28 バックアップ設定」を参照ください。

- **リストア**

リストアに関する設定を行うには、リストア画面を使用します。
詳細は、「4.5.29 リストア」を参照ください。

- **アップデート**

アップデートに関する設定を行うには、アップデート画面を使用します。
詳細は、「4.5.30 アップデート」を参照ください。

5.5 管理

システムの管理を行います。

5.5.1 ハードウェア状態

ハードウェア状態では、現在のハードウェア状態を表示します。

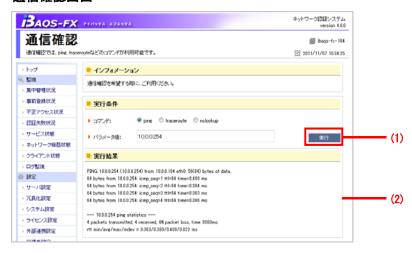
ハードウェア状態画面

ハードウェア状態画面の項目

番号	画面項目	説明
(1)	CPU	CPU の使用率です。
(2)	メモリ　used	メモリの使用率です。
(3)	メモリ　buffers	メモリのバッファ率です。
(4)	メモリ　cached	メモリのキャッシュ率です。
(5)	メモリ　free	メモリの空き率です。
(6)	スワップ	スワップの使用率です。
(7)	ディスク　ローカル	ローカルディスクの使用率です。
(8)	ディスク　ミラー	ミラーディスクの使用率です。

5.5.2 通信確認

通信確認では、ping や traceroute などのコマンドを利用して通信状況を確認することができます。

通信確認画面

通信確認画面の項目

番号	画面項目	説明
(1)	実行ボタン	コマンド（ping, traceroute, nslookup）を実行します。
(2)	実行結果	コマンドの実行結果を表示します。

5.5.3 オンラインマニュアル

オンラインマニュアルでは、管理画面の操作方法を PDF ファイルにて確認できます。

オンラインマニュアル画面

オンラインマニュアル画面の項目

番号	画面項目	説明
(1)	取扱説明書リンク	取扱説明書を表示します。

5.5.4 ログアウト

ログアウトでは、管理画面からログアウトします。

ログアウト画面

5.6 セカンダリ

iBAQS-FX では冗長構成時のスタンバイ状態にあるサーバをセカンダリ機と称します。セカンダリ機で利用できる画面は制限されています。

5.6.1 セカンダリ トップ

セカンダリトップでは、セカンダリ機の現在のシステム状況を表示します。

セカンダリトップ画面

セカンダリトップ画面の項目

番号	画面項目	説明
(1)	ライセンス有効期限	ライセンス有効期限です。
(2)	冗長化	冗長構成の状態です。 ➢ 通常運転中…正常に冗長構成で動作しています。 ➢ 縮退運転中…ピアサーバが存在しません。 ➢ 手動復旧待ち…ピアサーバと同期がとれていません。 ➢ 異常…ピアサーバとの接続に問題が発生しています。
(3)	ミラーディスク	ミラーディスクの状態です。 ➢ 通常同期中…正常にミラーリングを行っています。 ➢ 強制同期中(N%)…通常同期に加え、差分同期を行っています。
(4)	サービス状態	サービス状態です。 ➢ 正常動作中…すべてのサービスが正常に動作していま

		す。 ➢ 一部停止中…一部のサービスが停止しています。

5.6.2 セカンダリ サービス状態

セカンダリサービス状態では、セカンダリ機の各サービスの稼働状況を表示します。サービスが停止している場合は起動することができます。

セカンダリサービス状態画面

セカンダリサービス状態画面の項目

番号	画面項目	説明
(1)	NTP	NTP サービスです。 iBAQS-FX の時刻を NTP サーバに同期します。 NTP を有効にした場合に利用します。
	同期サービス	冗長構成時にミラーディスクを用意し、ピアサーバと常時同期します。 冗長構成に利用します。
	冗長監視サービス	フェイルオーバー対象のリソースを監視します。 冗長構成に利用します。
	UPS 制御サービス	UPS と通信を行い、連携を行うサービスです。 UPS 連携を行う場合に利用します。
	SNMP エージェントサービス	SNMP エージェントとして動作するサービスです。 SNMP マネージャ連携を行う場合に利用します。

5.6.3 セカンダリ サーバ設定

セカンダリサーバ設定では、セカンダリ機のサーバに関する設定を行います。セカンダリ機でネットワークに関する設定を変更することはできません。設定変更を行う場合は、冗長構成を解除してから行ってください。但し、時刻設定や再起動、シャットダウンは可能です。

セカンダリサーバ設定-基本画面

セカンダリサーバ設定-基本画面の項目

番号	画面項目	説明
(1)	使用 LAN インターフェース	使用するインターフェースです。 eth0 または eth1 を選択します。
(2)	eth[n] MAC アドレス	eth[n]の MAC アドレスです。
(3)	eth[n] 使用	eth[n]の使用状態です。
(4)	eth[n] IP アドレス	eth[n]の IP アドレスです。
(5)	eth[n] サブネットマスク	eth[n]のサブネットマスクです。
(6)	デフォルトゲートウェイ	サーバのゲートウェイです。
(7)	ホスト名	サーバのホスト名です。
(8)	セッションタイマー時間	セッションタイマー時間です。 管理画面の無操作によるタイムアウト時間を設定します。
(9) ～ (11)	DNS	DNS です。 オンラインでのライセンス設定、アップデート機能をご利用いただくためには DNS の設定が必須です。
(12) ～ (15)	タイムサーバ	NTP サーバです。 iBAQS-FX が時刻同期に使用する NTP サーバを設定します。
(16) (17)	プロキシサーバ	プロキシサーバです。 iBAQS-FX がアップデートサーバと通信する際に使用するプロキシサーバを設定します。

サーバ設定−時刻画面

サーバ設定<<時刻タ ブ>>画面の項目

番号	画面項目	説明
(1)	管理 PC	管理 PC の日時です。
(2)	入力	設定したい日時を入力します。
(3)	選択	管理 PC の日時か入力日時かを選択します。

サーバ設定−再起動画面

サーバ設定−シャットダウン画面

5.6.4 セカンダリ 冗長化設定

セカンダリ冗長化設定では、セカンダリ機の冗長化設定内容を表示します。変更を行うことはできません。変更したい場合は、冗長化を解除してから行ってください。

セカンダリ冗長化設定画面

セカンダリ設定画面の項目

番号	画面項目	説明
(1)	冗長化	冗長化設定状態です。「する」が表示されます。
(2)	通信インターフェース	ピアサーバと同期をとる際に利用するインターフェースです。
(3)	ピアサーバ IP アドレス	冗長化を構成するピアサーバの IP アドレスです。
(4)	仮想 IP アドレス	冗長構成時の仮想 IP アドレスです。
(5)	再構成方式	冗長化の再構成方式です。

5.6.5 セカンダリ ライセンス設定

セカンダリ機でのライセンスに関する設定を行うには、ライセンス設定画面を使用します。プライマリ機と同様の機能です。

詳細は、「4.5.4 ライセンス設定」を参照ください。

5.6.6 セカンダリ 外部連携設定

セカンダリ機での外部連携に関する設定を行うには、外部連携設定画面を使用します。利用可能な連携は、「UPS 連携」と「SNMP マネージャ連携」です。

詳細は、「4.5.5 外部連携設定」を参照ください。

5.6.7 セカンダリ 管理者設定

セカンダリ機での管理者に関する設定を行うには、管理者設定画面を使用します。利用可能な設定は、管理者 ID と管理者パスワード、アクセス制御です。

詳細は、「4.5.10 管理者設定」を参照ください。

5.6.8 セカンダリ ハードウェア状態

セカンダリ機でのハードウェア状態は、ハードウェア状態画面を使用します。プライマリ機と同様な機能です。

詳細は、「5.5.1 ハードウェア状態」を参照ください。

5.6.9 セカンダリ 通信確認

セカンダリ機での通信確認は、通信確認画面を使用します。プライマリ機と同様な機能です。

詳細は、「5.5.2 通信確認」を参照ください。

5.6.10 セカンダリ オンラインマニュアル

セカンダリ機でのオンラインマニュアルは、オンラインマニュアル画面を使用します。プライマリ機と同様な機能です。

詳細は、「5.5.3 オンラインマニュアル」を参照ください。

5.6.11 セカンダリ ログアウト

セカンダリ機でのログアウトは、ログアウト画面を使用します。プライマリ機と同様な機能です。

詳細は、「5.5.4 ログアウト」を参照ください。

5.7　利用者専用画面

iBAQS-FX では利用者専用の画面を準備しています。各用途に応じてご利用いただけます。

5.7.1　パスワード変更

パスワード変更では、利用者自らが認証用のパスワード変更を行うことができます。

【手順】

1.　以下の URL にアクセスします。

http://<iBAQS-FX の IP アドレス>:10080/

2.　認証ユーザーID と認証パスワードを入力して[ログイン]ボタンをクリックします。

3.　ログイン後、利用者メニューが表示され、「パスワード変更」リンクをクリックします。

4. パスワード変更画面で認証パスワードを入力して「変更」ボタンをクリックします。

➢ 認証パスワードに設定可能は文字は半角英数字と記号(. @ _ -)です。

5. これで設定変更完了です。

5.7.2 証明書手続き

証明書手続きでは、利用者自らがサーバ証明書のダウンロード、クライアント証明書の発行・失効・ダウンロードを行うことができます。

【手順】

1. 以下の URL にアクセスします。

http://<iBAQS-FX の IP アドレス>:10080/

2. 認証ユーザーID と認証パスワードを入力して[ログイン]ボタンをクリックします。
3. ログイン後、利用者メニューが表示され、「証明書のお手続き」リンクをクリックします。

4. 希望する操作を行います。

証明書手続き画面の項目

番号	画面項目	説明
(1)	状態	証明書の発行状態です。 ➢ 発行済み…証明書が発行済みです。 ➢ 未発行…証明書が未発行です。
(2)	発行／失効	証明書を発行／失効します。
(3)	ダウンロード	証明書をダウンロードします。 証明書が発行されている場合のみです。

5.7.3 事前登録

事前登録では、利用者自らが事前登録を行います。事前登録した情報を管理者の承認が許可された場合、クライアント情報に登録されます。

【手順】

1. 以下の URL にアクセスします。

http://<iBAQS-FX の IP アドレス>:10080/entry.jsp

2. 以下の項目を入力して[登録申請]ボタンをクリックします。

事前登録画面の項目

番号	画面項目	説明
(1)	認証パターン	認証パターンです。
(2)	利用者名	利用者名です。
(3)	PC 名	PC 名です。
(4)	通信機器	通信機器の MAC アドレスおよび IP アドレスです。
(5)	ユーザーID	ユーザーID です。
(6)	メールアドレス	メールアドレスです。
(7)	トークンパスワード生成桁数	ソフトウェアトークンの生成するパスワードの桁数です。
(8)	トークン乱数キー	ソフトウェアトークンがワンタイムパスワードを生成する際に利用する乱数キー（シード）です。

- iBAQS-FX と同一セグメントにいる場合には、現在アクセスしている通信機器の IP アドレスと MAC アドレスが自動取得されます。

- 認証モード時に未登録端末を事前登録したい場合は、登録済みの端末を利用して事前登録を行ってください。
- 事前登録完了後、管理画面の「事前登録状況」画面から承認処理を行ってください。

⚠

- iBAQS-FX と同一セグメント以外からのアクセスの場合には、MAC アドレスが自動取得されません。また、選択項目も表示されません。
- 「システム設定」<<基本>>で事前登録 IP アドレスを指定しないに設定している場合には、IP アドレスは登録されません。

5.7.4 証明書かんたんインストール利用申請

証明書かんたんインストール利用申請では､利用者自らがメールアドレスを入力して証明書かんたんインストールを利用するための申し込みを行うことが出来ます。

【手順】

1. 以下の URL にアクセスします。

http://<iBAQS-FX の IP アドレス>:10080/request.jsp

2. メールアドレスを入力して[申請]ボタンをタップします。
3. 利用案内メールが送信されます。利用案内メールに記載されている URL を開くと証明書かんたんインストールを利用することが出来ます。

5.7.5 証明書かんたんインストール

証明書かんたんインストールでは、モバイルデバイスへの証明書インストールを支援する機能を提供します。

【手順】

1. 証明書かんたんインストール利用案内画面から管理者が送付した利用案内メールまたは利用申請によって送付されたメールの URL を開きます。

2. 証明書かんたんインストール画面が表示されます。[認証局証明書]ボタン（iOS デバイスのみ)、[クライアント証明書]ボタンをタップすると証明書のインストールを行うことが出来ます。Android デバイス以外ではインポートパスワードをタップすると選択状態になるので、もう一度タップしてコピーしてください。Android デバイスの場合にはロングタップで表示されるメニューから[すべて選択]を選んで、選択範囲をロングタップで表示されるメニューあら[コピー]を選んでください。

3. 証明書かんたんインストール初回利用時に証明書かんたんインストール画面への URL が利用者へメールで送信されます。本メールに記載されている URL の有効期間は「認証局設定」<<証明書かんたんインストール>>の URL 有効期間で変更可能です。有効期限が切れた場合には再度申請手続きが必要です。

5.7.6 設定ナビ

設定ナビでは､証明書かんたんインストール利用者へモバイルデバイスの証明書利用設定を案内することが可能です。

【手順】

1. 証明書かんたんインストール画面の設定ナビボタンをタップします。

2. 設定ナビ画面が表示されます。画面に従ってアプリケーションの設定を行います。

5.7.7 トークン設定内容

トークン設定内容では、ソフトウェアトークンの設定内容を確認する事が可能です。

【手順】

1. 証明書かんたんインストール利用案内画面から管理者が送付した利用案内メールの URL を開きます。

2. ユーザーID、トークン乱数キー、パスワード桁数が表示されます。トークン乱数キーはロングタップでコピーする事が可能です。

3. ソフトウェアトークンにトークン乱数キー、パスワード桁数を設定します。

5.8 認証スイッチ設定例

認証スイッチの設定例を示します。

※以下のスイッチは、アライドテレシス社製品です。

5.8.1 CentreCOM 8300/8400/8600/8700 シリーズ

■ ＭＡＣベース認証

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[iBAQS-FX の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=MACBASED
ENABLE PORTAUTH=MACBASED PORT=[ポート番号]
```

■ IEEE802.1X 認証

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[iBAQS-FX の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=8021X
ENABLE PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR
```

5.8.2 CentreCOM 9400 シリーズ

■ ＭＡＣベース認証

```
SET IP LOCAL INTERFACE=[vlan-if]
ADD RADIUSSERVER SERVER=[iBAQS-FX の IP アドレス] ORDER=1 PORT=1812 ACCPORT=1813 SECRET=[共有パスワ
ード]
ENABLE PORTAUTH
SET PORTAUTH=MACBASED PORT=[ポート番号] TYPE=AUTHENTICATOR REAUTHENABLED=DISABLED
```

■ IEEE802.1X 認証

```
SET IP LOCAL INTERFACE=[vlan-if]
ADD RADIUSSERVER SERVER=[iBAQS-FX の IP アドレス] ORDER=1 PORT=1812 ACCPORT=1813 SECRET=[共有パスワ
ード]
ENABLE PORTAUTH
SET PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR REAUTHENABLED=DISABLED
```

5.8.3 CentreCOM 8900/9900 シリーズ

■ ＭＡＣベース認証

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[IBAQS-FX の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=MACBASED
ENABLE PORTAUTH=MACBASED PORT=[ポート番号]
```

■ IEEE802.1X 認証

```
SET IP LOCAL=1 IPADDRESS=[IP アドレス]
ADD RADIUS SERVER=[IBAQS-FX の IP アドレス] SECRET=[共有パスワード] PORT=1812 ACCPORT=1813 LOCAL=1
ENABLE PORTAUTH=8021X
ENABLE PORTAUTH=8021X PORT=[ポート番号] TYPE=AUTHENTICATOR
```

5.8.4 x200/x210/x510/x600/x610/x900 シリーズ

■ ＭＡＣベース認証

```
ip radius source-interface [IP アドレスまたは IFNAME]
radius-server host [iBAQS-FX の IP アドレス] key [共有パスワード]
aaa authentication auth-mac default group radius
interface [ポート番号]
auth-mac enable
```

■ IEEE802.1X 認証

```
ip radius source-interface [IP アドレスまたは IFNAME]
radius-server host [iBAQS-FX の IP アドレス] key [共有パスワード]
aaa authentication dot1x default group radius
interface [ポート番号]
dot1x port-control auto
```

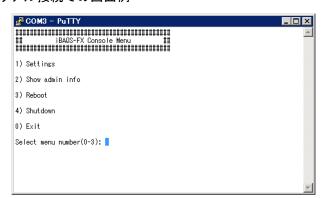
5.9 コンソールメニュー

コンソールメニューではCUIによる簡易的なサーバの操作が可能です。
接続は以下の方法をサポートしています。

接続方法	要件
サーバコンソール	モニタ(アナログ接続、iBAQS-FX側はD-Sub 15pin) キーボード(USB接続)
シリアル接続	クロスケーブル(iBAQS-FX側はD-Sub 9pin) シリアルポートの付いているパソコン 通信速度115200bps
ssh接続	sshクライアントのインストールされたパソコン

操作可能な内容は以下の内容です。

操作内容	対象
サーバ設定確認	使用LAN I/F、冗長構成(有効/無効)、 I/F(有効/無効)、I/F(IPアドレス)、I/F(サブネットマスク)、デフォルトゲートウェイ、DNS
サーバ設定変更	I/F(有効/無効)、I/F(IPアドレス)、I/F(サブネットマスク)、デフォルトゲートウェイ、DNS
管理者情報確認	管理者ID、管理者パスワード
再起動	−
シャットダウン	−

シリアル接続での画面例

6 保守

iBAQS-FX の保守について説明します。

6.1 バックアップとリストア

iBAQS-FX のバックアップとリストアについて説明します。

バックアップ

バックアップを行います。

詳細は、「4.5.28 バックアップ設定」を参照してください。

リストア

リストアを行います。

詳細は、「4.5.29 リストア」を参照してください。

6.2 障害発生時の対応

iBAQS-FX の障害発生時の対応について説明します。

iBAQS-FX が何らかの障害で停止した場合、ネットワーク接続が不可となります。

暫定対応として一時的にネットワーク接続を確保するため、認証スイッチの認証設定を解除してください。

再起動しても障害事象が解決しない場合には、バックアップファイルを採取して販売店にお問い合わせください。

7 困った時には

iBAQS-FX を利用して困ったときの対処方法について説明します。

7.1 FAQ

iBAQS-FX の FAQ を示します。

1. 管理画面にアクセスできません

→ iBAQS-FX に PING が通ることを確認してください。

デフォルトの IP アドレスは以下の通りです。

IP アドレス	192.168.1.1

→ URL が誤っていないことを確認してください。

管理画面への URL は以下の通りです。

http://<サーバ IP アドレス>:10080/

2. 管理画面にログインできません

→ 管理者の ID とパスワードを確認してください。

デフォルトの値は以下の通りです。

ID	manager
パスワード	friend

3. 認証が行えません

→ ネットワーク機器との疎通ができているか確認してください。

→ ネットワーク機器設定が誤っていないか確認してください。

ネットワーク機器の IP アドレスや共有パスワードを確認してください。

4. 冗長化設定ができません

→ ピアサーバとの通信が行えるか確認してください。

7.2 サポートセンター

以下の窓口にお問い合わせください。

iBAQS-FX 担当

アイビーソリューション株式会社

〒918-8152 福井県福井市今市町 66-20-2 ホクコンビル 4F

TEL：0776-38-6373　　　FAX：0776-38-5341

URL　http://www.ib-sol.co.jp

e-mail：support.ibaqs@ib-sol.co.jp

〈受付時間〉

9:00 ～12:00、13:00 ～ 17:00　月～金（祝・祭日を除く）

Rev.20150810　　アイビーソリューション株式会社